

# **Index**

- 1. ISMS Policy**
- 2. Document Control Policy**
- 3. Access Control Policy**
- 4. Password Security Policy**
- 5. Backup Policy**
- 6. Incident Response Policy**
- 7. Data Security Policy**
- 8. Network Management Policy**
- 9. Vulnerability Management Policy**
- 10. Risk Management Policy**
- 11. Asset Management Policy**
- 12. Clear Desk Clear Screen Policy**
- 13. Organization structure**
- 14. Acceptable Use Policy**
- 15. Fire Safety Plan and Evacuation Policy**
- 16. System Security Policy**
- 17. Internet Access Policy**
- 18. E-mail Access Policy**
- 19. Malware Protection Policy**
- 20. Log Management Policy**
- 21. Encryption Policy**
- 22. Change\_Management\_Policy**



# Information Security Management System Policy

Document No. GIPCL/PL/01

Release Date: 23<sup>rd</sup> May 2020

# Information Security Management System Policy

	<b>Information Security Management System Policy</b>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020



**This document is the property of  
Gujarat Industries Power Co. Ltd.**

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujrat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<b>Information Security Management System Policy</b>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

## Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release

	<b>Information Security Management System Policy</b>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

## Table of Contents

1	Purpose .....	5
2	Scope.....	5
3	ISMS Policy .....	5
3.1	Scope of the ISMS.....	5
3.2	Information Security Requirements .....	5
3.3	Top Management Leadership & Commitment.....	6
3.4	Management Representative .....	6
3.5	Framework for Setting Objectives and Policy .....	6
3.6	Roles and Responsibilities.....	7
3.7	Continual Improvement Policy.....	7
3.8	Approach to Managing Risk .....	9
3.9	Human Resources.....	9
3.10	Auditing and Review.....	9
3.11	Documentation Structure and Policy.....	11

	<h1>Information Security Management System Policy</h1>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

## 1 Purpose

The Information Security Management System Policy (hereafter referred to as “ISMS Policy”) is a required document which acts as the root “Quality Manual” of the Information Security Management System (ISMS).

This policy defines how Information Security will be set up, managed, measured, reported on and developed within GIPCL.

The International Standard for Information Security, BS ISO/IEC 27001:2013 (referred to in this document as ISO/IEC 27001), is a development of the earlier British Standard, BS 7799.

GIPCL has decided to pursue full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an external third party.

## 2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GIPCL business or interact with internal networks and business systems, whether owned or leased by GIPCL, the employee, or a third party.

This policy applies to employees, contractors, consultants, temporaries, and other workers at GIPCL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by GIPCL.

## 3 ISMS Policy

### 3.1 Scope of the ISMS

For the purposes of certification within GIPCL, the boundaries of the Information Security Management System are defined as follows:

[SIR Define the scope of the ISMS in terms of the characteristics of the business, the organisation, its location, assets and technology. Include details of and justification for any exclusions from the scope.]

### 3.2 Information Security Requirements

A clear definition of the requirements for information security will be agreed and maintained with the business so that all ISMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory and contractual requirements will also be documented and input to the planning process. Specific requirements with regard to the security of new or changed systems or services

	<h2>Information Security Management System Policy</h2>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

will be captured as part of the design stage of each project.

It is a fundamental principle of the GIPCL Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

### 3.3 Top Management Leadership & Commitment

Commitment to information security extends to senior levels of the organisation and will be demonstrated through this ISMS Policy and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality objectives are being met and quality issues are identified through the audit programme and management processes. Management Review can take several forms including departmental and other management meetings.

### 3.4 Management Representative

The [Information Security Manager] shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

- The identification, documentation and fulfilment of information security requirements
- Implementation, management and improvement of risk management processes
- Integration of processes
- Compliance with statutory, regulatory and contractual requirements
- Reporting to top management on performance and improvement

### 3.5 Framework for Setting Objectives and Policy

An annual cycle will be used for the setting of objectives for information security, to coincide with the budget planning cycle. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, informed by the annual management review with stakeholders.

ISMS objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on a quarterly basis to ensure that they remain

	<b>Information Security Management System Policy</b>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

valid. If amendments are required, these will be managed through the change management process.

In accordance with ISO/IEC 27001:2013 the control objectives and policy statements detailed in Annex A of the standard will be adopted where appropriate by GIPCL. These will be reviewed on a regular basis in the light of the outcome from risk assessments and in line with Information Security Risk Treatment Plan. For references to the controls that implement each of the policy statements given please, see Statement of Applicability.

### 3.6 Roles and Responsibilities

Within the field of information security, there are a number of management roles that correspond to the areas defined within the scope set out above. In a larger organisation, these roles will often be filled by an individual in each area. In a smaller organisation these roles and responsibilities must be allocated between the members of the team.

It is the responsibility of the [Information Security Manager] to ensure that staff understand the roles they are fulfilling and that they have appropriate skills and competence to do so.

### 3.7 Continual Improvement Policy

GIPCL policy with regard to Continual Improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Make information security processes and controls more measurable in order to provide a sound basis for informed decisions
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings with stakeholders and document them in a Continual Improvement Plan
- Review the Continual Improvement Plan at regular management meetings in order to prioritise and assess timescales and benefits



	<b>Information Security Management System Policy</b>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

Ideas for improvements may be obtained from any source including employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be added to the Continual Improvement Plan and evaluated by the staff member responsible for Continual Service Improvement.

	<h2>Information Security Management System Policy</h2>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

As part of the evaluation of proposed improvements, the following criteria will be used:

- Cost
- Business Benefit
- Risk
- Implementation timescale
- Resource requirement

If accepted, the improvement proposal will be prioritised in order to allow more effective planning.

### 3.8 Approach to Managing Risk

Risk management will take place at several levels within the ISMS, including:

- Management planning - risks to the achievement of objectives
- Information security and IT service continuity risk assessments
- Assessment of the risk of changes via the change management process
- As part of the design and transition of new or changed services

High level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision.

Refer Risk Management Policy for more details.

### 3.9 Human Resources

GIPCL will ensure that all staff involved in information security are competent on the basis of appropriate education, training, skills and experience.

The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill levels within GIPCL. Training needs will be identified and a plan maintained to ensure that the necessary competencies are in place.

Training, education and other relevant records will be kept by the HR Department to document individual skill levels attained.

### 3.10 Auditing and Review

Once in place, it is vital that regular reviews take place of how well information security processes and procedures are being adhered to. This will happen at three levels:

- Structured regular management review of conformity to policies and procedures
- Internal audit reviews against the ISO/IEC 27001 standard by the GIPCL Quality Team
- External audit against the standard in order to gain and maintain certification

Details of how internal audits will be carried out can be found in Internal Audit Process.



# Information Security Management System Policy

Document No. GIPCL/PL/01

Release Date: 23<sup>rd</sup> May 2020

	<b>Information Security Management System Policy</b>	Document No. GIPCL/PL/01
		Release Date: 23 <sup>rd</sup> May 2020

### 3.11 Documentation Structure and Policy

All information security policies and plans must be documented. This section sets out the main documents that must be maintained in each area.

Details of documentation conventions and standards are given in the Document Control Policy.

A number of core documents has been created and will be maintained as part of the ISMS. They are uniquely numbered and the current versions are tracked in Master List of Documents.



## Document Control Policy

Document No. GIPCL/PL/02

Release Date: 23<sup>rd</sup> May 2020

# Document Control Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Document Control Policy</h2>	Document No. GIPCL/PL/02
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
4.1	Preparation & Review of the document.....	4
4.2	Approval of the document.....	5
4.3	Release of the document .....	5
4.4	Archival/Retention of documents .....	6
4.5	Control of Records.....	6

	<h1>Document Control Policy</h1>	Document No. GIPCL/PL/02
		Release Date: 23 <sup>rd</sup> May 2020

## 1 Overview

The ISO/IEC 27001 standard requires that all documents that make up the Information Security Management System (ISMS) must be controlled. Such control is essential in order to ensure that the correct processes and procedures are in use at all times within the organisation and that they remain appropriate for the purpose for which they were created.

The general principles are that all documented information must be:

- Readily identifiable and available
- Dated, and authorised by a designated person
- Legible and readable
- Maintained under version control and available to all locations where service management activities are performed
- Promptly withdrawn when obsolete and retained in/as an archive where required for legal or knowledge preservation purposes, or both

This procedure sets out how this level of control will be achieved within GIPCL.

## 2 Purpose

This process explains the set of activities needed to initiate, analyze, prepare, review, approve and release a new / existing document within the purview of the ISMS of the organization.

## 3 Scope

This policy applies to all the documented information created during the business processes.

## 4 Policy

Requirement to release/review a policy can arise from the following events

- Suggestions / Problems raised by any employee through mail / helpdesk / discussions
- Internal ISMS Audit / External Audit findings/Network Audit
- Minutes of Security Council Meeting

This implies to the set of activities needed to initiate, analyse, prepare, review, approve and release a new / existing document.

### 4.1 Preparation & Review of the document

- Based on the Inputs as stated above, requirement for new or change in existing document can



	<h1>Document Control Policy</h1>	<p>Document No. GIPCL/PL/02</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	----------------------------------	-------------------------------------------------------------------------------------

arise.

- All documents shall be authored by the Document Owner
- Template for ISMS processes is available that should be used for all ISMS Process definitions.
- After a document is prepared/ revised, the document shall be given for review. The reviewer may be respective Security Council Member, Reporting officer or as identified by ISMS Officer / CISO.
- The reviewer shall give his comment either through mail or on the document itself.
- After review, the document shall be given back to the author with observations.
- After reviewing the observation, author shall incorporate the changes. The steps defined above are repeated till the reviewer approves the document.
- In case any minor changes (for example: Error in template, formula mistake etc.), are required changes can be done by ISMS administrator. However, no review records shall be maintained.
- All ISMS Processes, Implemented Policies will be reviewed at least once in a year.

## 4.2 Approval of the document

- After review, the document will be forwarded to ISMS Officer / CISO who shall approve the document. If any changes are suggested, then the document is sent back to the document owner and tasks in Section 4.1 are repeated till the document gets the final approval from the ISMS Officer / CISO.

## 4.3 Release of the document

- When a new process document is released, an entry is made in the Master List of ISMS Processes.
- When a new guideline is released, an entry is made in the Master List of ISMS Processes. Any other new release will have entry in appropriate folder.
- Whenever a new document is released for the first time, it is assigned version no. V1.0. In case an existing document is revised, escalate version no by 0.1 for minor changes and for major changes round off the version number to the next whole digit number (eg. if the current version number of the document is 2.2 and a minor change occurs, then the version number will escalate to 2.3 and if a major change occurs, then the version number will switch to 3.0). Only 9 minor versions can be released for a template/format. A major version should necessarily be released after 9 minor versions, but a major version can also be released whenever appropriate (Major & Minor changes refers to the impact of the change on the document which can be decided by the ISMS Officer / CISO or ISMS Administrator at their

	<h2>Document Control Policy</h2>	<p>Document No. GIPCL/PL/02</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	----------------------------------	-------------------------------------------------------------------------------------

discretion).

### Document Naming Convention

GIPCL\_DocumentIdentifier No\_DocName

#### Document Identifier

- PL corresponds to policy
- PR Corresponds to process

#### 4.4 Archival/Retention of documents

- The Soft copies of all the obsolete documents shall be kept in a separate sub folder named “Obsolete Documents” in the ISMS folder on the server. Thus, it is ensured that only the current version of ISMS is available to all concerned.

#### 4.5 Control of Records

- All records pertaining to individual processes are maintained by respective Document Owners or people identified by them. The custodian of the records (i.e. respective Document Owners or people identified by them) makes sure that the records are legible, readily identifiable and retrievable.



## Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

# Access Control Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Access Control Policy</h2>	Document No. GIPCL/PL/03
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
4.1	Business Requirements of Access Control .....	4
4.2	User Access Management .....	5
4.3	User Registration and Deregistration .....	5
4.4	User Access Provisioning .....	7
4.5	Removal or Adjustment of Access Rights .....	7
4.6	Management of Privileged Access Rights .....	7
4.7	User Authentication for External Connections.....	8
4.8	Supplier Remote Access to the Organisation Network.....	8
4.9	Review of User Access Rights .....	8
4.10	User Authentication and Password Policy .....	9
4.11	User Responsibilities .....	10
4.12	System and Application Access Control .....	12



# Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

The control of access to our information assets is a fundamental part of a defence in depth strategy to information security. If we are to effectively protect the confidentiality, integrity and availability of classified data then we must ensure that a comprehensive mix of physical and logical controls are in place.

## 2 Purpose

The Access Control Policy is an overarching document that is intended to establish the principles upon which many of the controls within this section of the standard are based.

## 3 Scope

This policy applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to GIPCL systems.

## 4 Policy

### 4.1 Business Requirements of Access Control

The control of access to our information assets is a fundamental part of a defence in depth strategy to information security. If we are to effectively protect the confidentiality, integrity and availability of classified data then we must ensure that a comprehensive mix of physical and logical controls are in place.

But our policy with regard to access control must ensure that the measures we implement are appropriate to the business requirement for protection and are not unnecessarily strict. The policy therefore must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved.

These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation that may apply e.g. the Data Protection Act, Sarbanes Oxley
- The regulatory framework in which the organisation and the system operates

	<h1>Access Control Policy</h1>	<p>Document No. GIPCL/PL/03</p> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	--------------------------------	-------------------------------------------------------------------------------

- Contractual obligations to external third parties
- The threats, vulnerabilities and risks involved
- The organisation’s appetite for risk

Business requirements should be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

In addition to the specific requirements, a number of general principles will be used when designing access controls for GIPCL systems and services. These are:

- Defence in Depth - security should not depend upon any single control but be the sum of a number of complementary controls
- Least Privilege - the default approach taken should be to assume that access is not required, rather than to assume that it is
- Need to Know - access is only granted to the information required to perform a role, and no more
- Need to Use - Users will only be able to access physical and logical facilities required for their role

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

## 4.2 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

## 4.3 User Registration and Deregistration



## Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

A request for access to the organisation's network and computer systems must first be submitted to the IT Service Desk for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorisation is obtained prior to user account creation. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account will have a unique user name that is not shared with any other user and is associated with a specific individual i.e. not a role or job title. Generic user accounts i.e. single accounts to be used by a group of people should not be created as they provide insufficient allocation of responsibility.

An initial strong password should be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves the organisation under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the IT Service Desk.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organisation prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution should especially apply in the case where the individual concerned has privileged access rights e.g. domain admin.

User accounts should be initially suspended or disabled only and not deleted. User account names should not be reused as this may cause confusion in the event of a later investigation.





## Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

### 4.4 User Access Provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general this should be role-based i.e. a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles should be maintained in line with business requirements and any changes to them should be formally authorised and controlled via the change management process.

Ad-hoc additional permissions should not be granted to user accounts outside of the group role; if such permissions are required this should be addressed as a change and formally requested.

### 4.5 Removal or Adjustment of Access Rights

Where an adjustment of access rights or permissions is required e.g. due to an individual changing role, this should be carried out as part of the role change. It should be ensured that access rights no longer required as part of the new role are removed from the user account. In the event that a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role should be requested via change management. Due consideration of any issues of segregation of duties should be given.

Under no circumstances should administrators be permitted to change their own user accounts or permissions.

### 4.6 Management of Privileged Access Rights

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users (such as IT support staff) should not make day to day use of user accounts with privileged access, rather a separate “admin” user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual e.g. “John Smith Admin”; generic admin accounts should not be used as they provide insufficient identification of the user.

	<h1>Access Control Policy</h1>	Document No. GIPCL/PL/03
		Release Date: 23 <sup>rd</sup> May 2020

Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

The use of user accounts with privileged access in automated routines such as batch or interface jobs should be avoided where possible. Where this is unavoidable the password used should be protected and changed on a regular basis.

#### 4.7 User Authentication for External Connections

In line with the network security policy the use of modems on non-organisation owned PCs or devices connected to the organisation’s network can seriously compromise the security of the network. Specific approval must be obtained from the IT Service Desk before connecting any equipment to the organisation’s network as per ISMS12004 Bring Your Own Device Policy.

Where remote access to the network is required via VPN, a request must be made via the IT Service Desk. A policy of using two factor authentication for remote access should be used in line with the principle of “something you have and something you know” in order to reduce the risk of unauthorised access from the Internet.

#### 4.8 Supplier Remote Access to the Organisation Network

Partner agencies or 3rd party suppliers must not be given details of how to access the organisation’s network without permission from the IT Service Desk. Any changes to supplier’s connections (e.g. on termination of a contract) must be immediately sent to the IT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by the IT Service Desk.

Partners or 3rd party suppliers must contact the IT Service Desk on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and user accounts must be disabled when not in use.

#### 4.9 Review of User Access Rights

On a regular basis (at least annually) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:

	<h1>Access Control Policy</h1>	<p>Document No. GIPCL/PL/03</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	--------------------------------	-------------------------------------------------------------------------------------

- People who should not have access (e.g. leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification e.g. generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed according to a formal procedure and any corrective actions identified and carried out.

A review of user accounts with privileged access will be carried out by the [Information Security Manager] on a quarterly basis to ensure that this policy is being complied with.

#### 4.10 User Authentication and Password Policy

A strong password is an essential barrier against unauthorised access. Unfortunately this area is often proven to be the weak link in an organisation’s security strategy and a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometric techniques.

[Organisation Name]’s policy is to make use of additional authentication methods based on a risk assessment which takes into account:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

Use of multi-factor authentication methods should be justified on the basis of the above factors and securely implemented and maintained where appropriate.

Single Sign-On (SSO) will be used within the internal network where supported by relevant systems unless the security requirements are deemed to be such that a further logon is required.

Whether single or multi-factor authentication is used, the quality of user passwords should be enforced in all networks and systems using the following parameters:

Parameter	Value
Minimum length	8
Maximum length	16
Re-use cycle	Cannot be the same as any of the previous 32 passwords
Characters Required	At least one capital letter At least one symbol At least one number
Password similarity	New password cannot share more than three characters in the same position as the old password
Change Frequency	At least every 90 days
Account lockout	On 5 incorrect logon attempts
Account lockout action	Account must be re-enabled by IT Service Desk
Other controls	Password cannot contain the user name

Any exceptions to these rules must be authorised by the [Information Security Manager].

### 4.11 User Responsibilities

In order to exercise due care and try to ensure the security of its information, [Organisation Name] expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day to day roles. Many recent high profile security breaches have been largely caused by unauthorised access to user accounts resulting from passwords being stolen or guessed.

It is vital therefore that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organisation.

In order to maximise the security of our information every user must:

- Use a strong password i.e. one which is in line with the rules set out in this policy



## Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically e.g. in a file or email
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended connected to the network is locked or logged out
- Leave nothing on display that may contain access information such as login names and passwords
- Inform the IT Service Desk of any changes to their role and access requirements

Failure to comply with these requirements may result in the organisation taking disciplinary action against the individual(s) concerned.



## Access Control Policy

Document No. GIPCL/PL/03

Release Date: 23<sup>rd</sup> May 2020

### 4.12 System and Application Access Control

As part of the evaluation process for new or significantly changed systems, requirements for effective access control should be addressed and appropriate measures implemented.

These should consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of permissions to objects (e.g. files, programs, menus) of different types (e.g. read, write, delete, execute) to subjects (user accounts and groups)
- Provision of varying views of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls such as
  - Non-display of password as it is entered
  - Account lockout once number of incorrect logon attempts exceeds a specified threshold
  - Provide information about number of unsuccessful logon attempts and last successful logon once user has successfully logged on
  - Date and time-based logon restrictions
  - Device and location logon restrictions
- User inactivity timeout
- Password management, including
  - Ability for user to change password
  - Controls over acceptable passwords
  - Password expiry
  - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Access to utility programs that provide a method of bypassing system security (e.g. data manipulation tools) should be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of a named project or change.



## Password Security Policy

Document No. GIPCL/PL/04

Release Date: 23<sup>rd</sup> May 2020

# Password Security Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Password Security Policy</h2>	Document No. GIPCL/PL/04
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
	General Guidelines .....	4
4.1	Password Construction .....	5
4.2	Storage and Management of Critical Password .....	5
4.3	Application Development .....	6
4.4	Prohibited User / Practices.....	6



# Password Security Policy

Document No. GIPCL/PL/04

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

Access to information and information systems shall be according to least privilege and need to know basis. The procedure shall be administered to ensure that the appropriate level of access control is applied to protect the information in each application or systems from unauthorized access, modification, disclosure or destruction to ensure that information accurate, confidential and is available when required.

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network. This guideline provides best practices for creating secure passwords.

All users, including contractors and vendors with access to GIPCL systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## 2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

## 3 Scope

This policy applies to employees, contractors, consultants, temporary and other workers at GIPCL including all personnel affiliated with third parties. It is applying to all application and systems used over GIPCL network.

## 4 Policy

### General Guidelines

- 1) All user passwords (individual as well as administrators) shall remain confidential and shall not be shared, posted or otherwise divulged in any manner.
- 2) An initial password shall be provided to the users securely during user creation password. The users shall change initial password after first login.



# Password Security Policy

Document No. GIPCL/PL/04

Release Date: 23<sup>rd</sup> May 2020

## 4.1 Password Construction

Following password construction policy shall be enforced for all users and administrative accounts on operating systems, applications, databases and all other information protected by password control.

- Password composition = alphanumeric and at least one special character
- Minimum password length = 8
- Maximum password age = 45 days
- Password history = 5
- Inactivity period for password lockout = 60 days
- Account lockout after 5 invalid attempts

Due to system limitations or business necessity if any of the password and account policy parameters cannot be followed, specific mechanisms shall be put in place to obtain approvals and implement countermeasures to mitigate the risk of not following the password policy.

Where it is not possible to implement individual user-ids and passwords within the application itself (due to design parameters), alternative solutions for restricting and auditing access privileges shall be evaluated for feasibility and shall be implemented. As far as possible, GIPCL shall not make do with the concept of utilizing the same user-id and password for all users.

## 4.2 Storage and Management of Critical Password

Below listed tables explains what type of passwords are called critical passwords. These passwords should be carefully managed to ensure that these passwords are not forgotten or are not lost.

System	Types of Passwords
Operating Systems	Administrator Password(s)
Information Systems / Business Applications	Super User Password (where available) Administrator Password System Password (for Database connectivity) where available
Databases	Database Super User Password Database Administrator Password Database Security Officer Password

	<h1>Password Security Policy</h1>	Document No. GIPCL/PL/04
		Release Date: 23 <sup>rd</sup> May 2020

Manual procedures for handling critical passwords are mentioned below:

**Storage of Critical Passwords:** The Corporate IT head should ensure that holders of critical passwords mentioned above place a written copy of the User-ID and password in a sealed tamper proof envelope specially developed for this purpose.

**Content of the Password Envelopes:** The following information should be documented on the face of the envelope: -

- User Name, department and designation
- Name / Identity of the Application, Operating System or Database for which the password has been lodged.

### 4.3 Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.

### 4.4 Prohibited User / Practices

- 1) Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential GIPCL information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.
- 2) Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
- 3) Passwords must not be revealed over the phone to anyone.
- 4) Do not reveal a password on questionnaires or security forms.
- 5) Do not hint at the format of a password (for example, "my family name").
- 6) Do not share GIPCL and its subsidiaries passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- 7) Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- 8) Do not use the "Remember Password" feature of applications (for example, web browsers).
- 9) Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

	<h2>Password Security Policy</h2>	Document No. GIPCL/PL/04 Release Date: 23 <sup>rd</sup> May 2020
-----------------------------------------------------------------------------------	-----------------------------------	---------------------------------------------------------------------

**On violations of this policy, management may take appropriate disciplinary action.**



# Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

# Backup Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Backup Policy</h2>	Document No. GIPCL/PL/05
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
	General Guidelines .....	<b>Error! Bookmark not defined.</b>
4.1	Password Construction .....	<b>Error! Bookmark not defined.</b>
4.2	Storage and Management of Critical Password .....	5
4.3	Application Development .....	<b>Error! Bookmark not defined.</b>
4.4	Prohibited User / Practices.....	6





# Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

To meet the enterprise business objectives and ensure continuity of its operations, GIPCL adopts and follow well-defined and time-tested plans and procedures, to ensure timely and reliable backup of its IT assets. The Backup Policy reiterates the commitment GIPCL delivering the fastest transition and highest quality of services through the backup arrangement ensuring that its customers, business activities and services do not suffer in any way. The policy shall be available with the CISO and BCP (Business Continuity Plan) team members of GIPCL.

## 2 Purpose

The purpose of this document is to set out the way in which backups of servers are carried out, including:

- Frequency of backups
- Types of backups
- Timing of backups
- What is backed up
- How tapes are used and managed
- Arrangements for offsite storage of tapes
- Tape retention policy
- What regular reports are produced?
- How disaster recovery information is saved

This document should be read in conjunction with the Service Continuity Plan which deals with how backups are used to restore data in the event of a disaster.

## 3 Scope

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to GIPCL systems.

## 4 Policy

### 4.1 Backup Method and Schedule

Backups are carried out using the Veritas NetBackup system which resides on the server ABC123. This software manages the process of saving data from each server to LTO2 tapes which are loaded in a



# Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

dual drive HP Ultrium2 tape library attached via a SCSI adapter to ABC123.

All servers are backed up nightly, six days a week according to the following schedule:

Night	Type of Backup
Monday	Incremental
Tuesday	Incremental
Wednesday	Incremental
Thursday	Incremental
Friday	Full

Backups are set to start at 20:00 each night. All local drives on each server are backed up. On the Exchange and SQL Server systems, additional data stores are also saved.

## 4.2 Tape Cycle

Backups are performed to a set of tapes for each night. These tapes are then removed the following working day morning, placed in a protective case and taken offsite. Based on current save volumes it is envisaged that one tape will be required per backup. LTO2 tapes hold 200Gb uncompressed and between 200-400Gb compressed. The following tape sets are used:

### Daily Sets

Daily tapes are reused after two weeks.

- MON1 (First Week)
- TUE1 (First Week)
- WED1 (First Week)
- THU1 (First Week)
- MON2 (Second Week)
- TUE2 (Second Week)
- WED2 (Second Week)
- THU2 (Second Week)

### Weekly Sets

Weekly tapes are reused after five weeks.

- WEEKLY1
- WEEKLY2
- WEEKLY3
- WEEKLY4

### Monthly Sets



# Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

Monthly tapes are reused after 60 weeks.

- MONTHLY1
- MONTHLY2
- MONTHLY3
- MONTHLY4
- MONTHLY5
- MONTHLY6
- MONTHLY7
- MONTHLY8
- MONTHLY9
- MONTHLY10
- MONTHLY11
- MONTHLY12

Assuming that one tape is sufficient per backup, this gives an overall requirement of 24 tapes.

## 4.3 Offsite Storage

Application developers must ensure that their programs contain the following security precautions:

The following tapes will be held offsite:

- 2 most recent daily backups
- 2 most recent weekly backups (which will at some points in the month include a MONTHLY backup)

The tapes will be held in a locked cabinet, with access to keys being restricted to:

[IT Department]

Tape Courier

Site Management

## 4.4 Tape Cycle Example

The following table shows how the above tape sets are used in a typical month. This example assumes no tapes are currently held offsite.

Date	Day	Tape Set	Tapes Taken Offsite	Tapes Returned
1	Mon	MON1		
2	Tue	TUE1	MON1	



## Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

Date	Day	Tape Set	Tapes Taken Offsite	Tapes Returned
3	Wed	WED1	TUE1	
4	Thu	THU1	WED1	MON1
5	Fri	WEEKLY1	THU1	TUE1
6	Sat			
7	Sun			
8	Mon	MON2	WEEKLY1	
9	Tue	TUE2	MON2	WED1
10	Wed	WED2	TUE2	THU1
11	Thu	THU2	WED2	MON2
12	Fri	WEEKLY2	THU2	TUE2
13	Sat			
14	Sun			
15	Mon	MON1	WEEKLY2	
16	Tue	TUE1	MON1	WED2
17	Wed	WED1	TUE1	THU2
18	Thu	THU1	WED1	MON1
19	Fri	WEEKLY3	THU1	TUE1
20	Sat			
21	Sun			
22	Mon	MON2	WEEKLY3	WEEKLY1
23	Tue	TUE2	MON2	WED1
24	Wed	WED2	TUE2	THU1
25	Thu	THU2	WED2	MON2
26	Fri	WEEKLY4	THU2	TUE2
27	Sat			
28	Sun			
29	Mon	MON1	WEEKLY4	WEEKLY2
30	Tue	TUE1	MON1	WED2
31	Wed	WED1	TUE1	THU2
1	Thu	THU1	WED1	MON1
2	Fri	MONTHLY1	THU1	TUE1
3	Sat			
4	Sun			



## Backup Policy

Document No. GIPCL/PL/05

Release Date: 23<sup>rd</sup> May 2020

Date	Day	Tape Set	Tapes Taken Offsite	Tapes Returned
5	Mon	MON2	MONTHLY1	WEEKLY3
6	Tue	TUE2	MON2	WED1
7	Wed	WED2	TUE2	THU1
8	Thu	THU2	WED2	MON2
9	Fri	WEEKLY1	THU2	TUE2
10	Sat			

### 4.5 Reporting

Reports will be produced on a weekly basis to track the volume of data being saved and the time taken to save it.

**On violations of this policy, management may take appropriate disciplinary action.**

	<h2>Incident Response Policy</h2>	Document No. GIPCL/PL/06
		Release Date: 23 <sup>rd</sup> May 2020

# Incident Response Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujarat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Incident Response Policy</h2>	Document No. GIPCL/PL/06
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Incident Response Policy

Document No. GIPCL/PL/06

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
	General Guidelines .....	4
4.1	Security Incident Management System.....	5
4.2	Reporting Information Security Events and Weakness .....	6
4.3	Management of Information Security Incident and Improvements .....	6
4.4	Disciplinary Process.....	8
4.5	Roles and Responsibilities Matrix (RACI) .....	8
4.6	Roles and Responsibilities .....	9





# Incident Response Policy

Document No. GIPCL/PL/06

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

To ensure that security incidents occurring to and misuse of Information assets / system, related support services and GIPCL facilities are detected, escalated and resolved in timely fashion and logged for further review.

## 2 Purpose

The purpose of this policy is to establish a standard for reporting, detection, escalation and resolving of incidents in a timely manner.

## 3 Scope

This policy document includes all type of incidents (as defined below) related to IT system/services/facilities and related support systems within GIPCL facilities.

## 4 Policy

### General Guidelines

- 1) All GIPCL employees shall report security incidents including security weaknesses, malfunctions, threats and security breaches immediately to Service Desk. A formal Incident Reporting and Management Procedure shall be in place to explain escalation levels in detail. All security incidents reported shall be recorded with its resolution and analysed by the Information Security.
- 2) GIPCL should manage incidents via Incident Management System. Users should immediately report all incidents pertaining to information security to Incident Management System/portal. The Incident Management System/portal should escalate all the incidents to functions (ITSD / Admin / HR / Information Security Team / Others) as per the relevancy of the incident.
- 3) A formal Incident Reporting and Management Procedure should be in place to explain escalation levels in detail.
- 4) Users shall not report to or discuss about incidents with other users or external persons. GIPCL shall have a formal process for the reporting of any incidents to the press, clients or security agencies like police.

	<h1>Incident Response Policy</h1>	<p>Document No. GIPCL/PL/06</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-----------------------------------	-------------------------------------------------------------------------------------

## 4.1 Security Incident Management System

**Security Incident:** All security violations, security weaknesses, software malfunctions, misuse of IT resources, violating GIPCL policies and procedures, applicable legal laws and any other event which has notable negative impact on the GIPCL’s Information systems shall be considered as Security Incidents.

**Examples of Incidents:** Below are the examples (but not limited to) of Incidents, which needs to be handled in GIPCL infrastructure:

- Malicious Attack;
- Information systems failures and loss of service;
- Breaches of confidentiality and integrity;
- Denial of service;
- Misuse of information systems;
- Password sharing;
- Misuse of internet/email;
- Theft of / damage to computer hardware equipment and communication network.

**Incident Management System:**

There should be an Incident management system in place. This incident management system will be a central repository of reported incidents. Users and Functions must report all the information security incidents using this system.

This Incident Management System will cater MIS reports from the incidents available in its database.

**Security Incident Response Team:**

An Incident Response Team shall be established to provide a quick, effective and orderly response to weaknesses/incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team’s mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving information / information generating systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. Information Security Team will coordinate these investigations.

	<h1>Incident Response Policy</h1>	<p>Document No. GIPCL/PL/06</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-----------------------------------	-------------------------------------------------------------------------------------

The Incident Security Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents.

Below are the members of Security Incident Response Team (SIRT):

Information Security Team

Representative from various departments (HR, Finance, Admin etc)

Where it is not possible to implement individual user-ids and passwords within the application itself (due to design parameters), alternative solutions for restricting and auditing access privileges shall be evaluated for feasibility and shall be implemented. As far as possible, GIPCL shall not make do with the concept of utilizing the same user-id and password for all users.

## 4.2 Reporting Information Security Events and Weakness

### Reporting Information Security Events

A formal information security reporting procedure shall be defined and implemented to ensure that information security events/incidents are reported responsibly, as quickly as possible. All users of GIPCL’s information systems shall be made aware of their responsibility to report any information security event/incident as quickly as possible by following the information security reporting procedure. The information security reporting procedure shall include:

The correct behaviour to be undertaken in case of a security incident covering:

- Reporting
- Handling
- Resolution
- Closure

### Reporting Security Weakness

All users of GIPCL’s information systems shall note and report any observed or suspected security weakness in the systems or IT services. Appropriate reporting mechanism shall be defined and implemented to facilitate reporting of suspected security weakness. Users shall not attempt to prove a suspected security weakness. The security incident can be reported to [informationsecurity@gipcl.com](mailto:informationsecurity@gipcl.com).

## 4.3 Management of Information Security Incident and Improvements

### Information Security Incident

All information security incidents shall be promptly investigated. Procedures and responsibilities shall be defined and documented to handle different types of information security incidents.

	<h1>Incident Response Policy</h1>	<p>Document No. GIPCL/PL/06</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-----------------------------------	-------------------------------------------------------------------------------------

Actions to recover from security incidents and correct system failures shall be carefully and formally controlled; in particular, the procedures shall ensure that:

- All information security incidents are recorded;
- Only authorized personnel with adequate knowledge/skills are allowed to access affected systems and data;
- Actions are taken to limit the effects of a security incident by isolating the problem as narrowly as possible;
- All emergency actions taken are documented in detail;
- The integrity of information systems and controls is confirmed with minimal delay;
- Suitable feedback is provided to the person/s who reported the information security incident after the incident has been dealt with and closed;

### **Learning from Information Security Incidents**

All information security incidents shall be analysed to identify:

- Recurring information security incidents;
- High impact incidents;
- Enhancements to existing controls or additional controls to be deployed to limit the frequency and impact of future occurrences;

The investigation shall provide sufficient information (including type, volume and cost of the incidents) so that management can take steps to ensure that:

The occurrence of such incidents are minimized or eliminated and Effective security controls have been implemented or re-established

### **Follow Up Analysis:**

A follow-up analysis will be performed after an incident has been fully handled and all systems are restored to a normal mode of operation.

The incident co-ordination team and other involved parties will meet and discuss actions that were taken and the lessons learnt.

### **Review and Records of Reported Incidents:**

During Information Security Steering Committee Review meeting, team members shall review all the incidents that have occurred and try to identify probable solutions to avoid their recurrence. The review shall be documented and records shall be maintained for the same. The findings shall be shared with relevant stakeholders, if required.

### **Collection of Evidence**

Incident Response Team shall be responsible for collection of evidence for the incidents/security breaches. The evidences may need to be collected for the investigation or root cause analysis. IRT shall be empowered to reset user password, check user system, collect evidence and disable user account till further notice. Incident Response Team shall be empowered to collect the evidences without any prior approval.

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

- Information describing all reported information security problems and violations must be retained for a period as per relevant jurisdiction(s).
- Regular analysis of reported information security incidents and violations.

#### 4.4 Disciplinary Process

A formal disciplinary process shall be in place for handling violations of Information Security Group policies and procedures.

Wherever possible, evidences shall be collected to initiate and support prosecution process for violating legal requirements (including GIPCL policies and procedures) and emphasis shall be given to ensure that these evidences are fully admissible in a court of law or GIPCL internal procedure.

For incidents causing violation of GIPCL policies and procedure, the matter shall be referred to HR by ITSD/Admin/IS team to initiate the disciplinary process and for violation of legal laws the matter shall be referred to legal department.

#### 4.5 Roles and Responsibilities Matrix (RACI)

Role Activity	Information Security	ISMS Steering Committee	Internal Users	External Users	Exempted
Authoring of this document	RA	CI	-	-	-
Review of this document	RA	CI	-	-	-
Approval of this document	I	RA	-	-	-

	<h1>Incident Response Policy</h1>	Document No. GIPCL/PL/06
		Release Date: 23 <sup>rd</sup> May 2020

Sign-off of this document	I	RA	-	-	-
Application of this document	RA	R	R	R	-

R	Responsible	This is the actual person who will carry out the task or articulate the subject.
A	Accountable	This is the person with whom the buck stops. The person who is accountable will more often than not (but not always) have someone in his or her team who is actually responsible for conducting that task or articulating that aspect.
C	Consulted	This is someone from whom the responsible individual must get an input or opinion. In other words, they have a say.
I	Informed	This is any person, including stakeholders and customers, who need to be made aware of this activity.

## 4.6 Roles and Responsibilities

### Information Security Team

- Policy ownership, development and maintenance.
- Compliance audit & risk reviews, Investigations needed.
- Shall respond to security incident and take immediate action to mitigate it.
- Shall maintain record of the incidents and analyze it for further review.
- Shall submit security incident analysis report to ISMS Steering Committee.
- Shall maintain evidence in secure manner for applicable retention period.
- Shall initiate the documenting process for future reference.
- Shall take approval from ISMS Steering Committee prior to use of organization held information for evidence collection.
- Conduct root cause analysis periodically on the recent past incidents.

### The Steering Committee:

- Shall review security incidents analysis report.
- Shall authorize and provide advice, before investigation is conducted.
- If criminal activity is suspected, should consider a referral to law enforcement agencies

	<h2>Incident Response Policy</h2>	<p>Document No. GIPCL/PL/06</p> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-----------------------------------	-------------------------------------------------------------------------------

### ITSD

- Incident Response.
- Shall record all incidents reported
- Shall escalate security incidents to appropriate individuals.
- Shall use security incident analysis to update knowledgebase and use it to respond to recurring incidents.

### Admin/Facility

- To respond and resolve Admin\Facility related incidents

### HR

- To respond and resolve HR related incidents
- Disciplinary Action

### Concerned Team:

- Prepare the corrective action plan for the incident.
- Shall coordinate with Information Security Manager in case of incident and take appropriate action to mitigate it.

### Users

- Shall report Security Incident immediately to Information Security Manager/Service Desk.
- Shall not shutdown/reboot machine or delete any file/application/program, in the event of security incident.
- Should not attempt to find a solution independently.

**On violations of this policy, management may take appropriate disciplinary action.**



## Data Security Policy

Document No. GIPCL/PL/07

Release Date: 23<sup>rd</sup> May 2020

# Data Security Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>



	<h2>Data Security Policy</h2>	Document No. GIPCL/PL/07
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
4.1	Definitions .....	4
4.2	Procedure .....	6
4.2.1	Use of Personal Data.....	6
4.2.2	Integrity of Personal Data .....	6
4.2.3	Notice.....	6
4.2.4	Access to Personal Data.....	7
4.2.5	Procedure for Accessing Personal Data .....	7
4.3	Security of Personal data .....	7
4.4	Transfer of personal data.....	7
4.5	Accountability .....	7
4.6	Procedure of enquiry/complaint.....	8

## 1 Overview

GIPCL Data Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

## 2 Purpose

This This Policy sets forth how GIPCL will manage the Personal Data that it collects in the normal course of business and ensure Information Security.

## 3 Scope

This Policy is applicable to GIPCL. Specifically, this Policy applies to:

- All individuals who provide Personal Data, such as Loan Applicants, Associates, Job Applicants, Contingent Workers, Interns, Retirees, Contractors, Customers, Business Partners, Shareholders, Directors and others;
- All locations where the Company operates, even where local regulations do not exist; and
- All methods of contact, including in person, written, via the Internet, direct mail, telephone, or facsimile.

This Policy is designed to inform all associates about their obligation to protect the privacy of all individuals (whether Loan Applicants, Associates, Job Applicants, Contingent Workers, Interns, Retirees, Contractors, Customers, Business Partners, Shareholders, Directors and others) and the security of their Personal Data.

## 4 Policy

This Policy does not necessarily describe how local management may handle Personal Data in order to comply with local regulations. Local management, in conjunction with the responsible human resources manager(s), will be responsible for accessing and complying with local regulations regarding the processing of Personal Data.

### 4.1 Definitions

Controller	Refers to the Company and its authorized third parties, which determine the purposes and means of processing of Personal Data.
------------	--------------------------------------------------------------------------------------------------------------------------------



## Data Security Policy

Document No. GIPCL/PL/07

Release Date: 23<sup>rd</sup> May 2020

Data Subject	Refers to any associate or third person (e.g., Loan Applicants, Associates, Job Applicants, Employees, Contingent Workers, Interns, Retirees, Contractors, Customers, Business Partners, Shareholders, Directors and others) who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
General Business Purpose	Defined as the Processing of Personal Data for any activity related to the commercial operations of the Company. This could include, but is not limited to, its sales and marketing; protecting intellectual property; the provision of services; internal operations; information technology and general employment matters, including recruitment both internally and externally. Data processing for General Business Purposes includes, but is not limited to, Loan Applicant's data, publishing directories, maintaining files, payroll processing, conducting performance reviews, and inter / intra-company communications
Personal Data	Defined as any information related to an identified or an identifiable person. For example, a Data Subject's home address, e-mail address, telephone number, or government-issued identification numbers would constitute Personal Data.
Processor	Defined as a natural or legal person, or any other entity that processes Personal Data on behalf of the Controller and under its control. In this context, a Processor may be its own employees or a payroll preparation firm that works on behalf of the Company and under its control etc. The Company requires Processors to protect the privacy, confidentiality and security of Personal Data.
Processing	Defined as any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

	<h1>Data Security Policy</h1>	Document No. GIPCL/PL/07
		Release Date: 23 <sup>rd</sup> May 2020

Sensitive Data	A subset of Personal Data, and refers to any Personal Data pertaining to racial or ethnic origins, trade union membership, medical or health conditions, political or religious beliefs, or criminal history.
Third Party	Defined as any natural or legal person, public authority, agency or any other entity other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data.

## 4.2 Procedure

### 4.2.1 Use of Personal Data

In the course of day-to-day business operations, authorized individuals within the Company may from time-to-time utilize and / or transfer Personal Data among various Company locations. These transfers of Personal Data are necessary in order to carry out the Company’s General Business Purposes.

Specifically, Personal Data may be used as follows:

- To identify a Data Subject personally;
- To communicate with a Data Subject;
- To manage the business.
- To comply with human resource requirements;
- To comply with government regulations;
- To provide associate benefits;

### 4.2.2 Integrity of Personal Data

The Company will take reasonable steps that Personal Data and Sensitive Data are:

- Obtained, where possible, directly from the Data Subject to whom the Personal Data relates;
- Obtained and processed fairly and lawfully by the Company for General Business Purposes;
- Relevant to and no more revealing than is necessary for General Business Purposes; and
- Kept up-to-date to maintain data accuracy on best effort basis, while data is under the control of the Company, and kept only for so long as is reasonably necessary.

### 4.2.3 Notice

	<h1>Data Security Policy</h1>	<p>Document No. GIPCL/PL/07</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-------------------------------	-------------------------------------------------------------------------------------

The Company informs Data Subjects about the purposes for which Personal Data is collected and used. In certain situations, Personal Data may be rendered anonymous so that the names of the Data Subjects are not known by Processors. In these cases, Data Subjects do not need to be notified.

#### 4.2.4 Access to Personal Data

The Company takes steps on best effort basis to make sure that the Personal Data it uses is correct. The Company will allow Data Subjects reasonable access to Personal Data about themselves during normal working hours and upon reasonable request, and will be allowed to update and / or correct any inaccurate information.

#### 4.2.5 Procedure for Accessing Personal Data

Questions about Personal Data and / or authorization to access such Personal Data are to be directed to Data Subject's concerned authority. Unauthorized access may be grounds for disciplinary actions, including termination.

### 4.3 Security of Personal data

The Company will take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access, disclosure, alteration and destruction. The Data in physical form will be kept at the storage location with limited access only to the concerned authority. The Data in Digital form will be stored in restricted storage space with limited access only to the concerned authority. Backup of Data in Digital Form will be kept at a location other than main storage location to protect from data loss.

### 4.4 Transfer of personal data

Subject to this Policy, the Company may from time-to-time transfer Personal Data within and between its various locations for General Business Purposes, in compliance with this Policy.

The Company's personnel, Directors, Shareholders, outside firms and consultants who receive Personal Data may be located in the Data Subject's home country or any other country in which the Company or its affiliates operate out of. Therefore, Personal Data may be transferred to any country in the world, including but not limited to India and other countries, and where the privacy laws may be more or less protective than the privacy laws where the Data Subjects live or work.

### 4.5 Accountability

The Company expects its employees, associates, independent contractors, subcontractors, and partners to maintain the trust placed in the Company by those Data Subjects who provide personal

	<h2>Data Security Policy</h2>	Document No. GIPCL/PL/07 Release Date: 23 <sup>rd</sup> May 2020
-----------------------------------------------------------------------------------	-------------------------------	---------------------------------------------------------------------

information to the Company. The Company may periodically audit privacy compliance, and where necessary, will extend by contract its privacy policies and data protection practices to the Company's supplier and partner relationships.

#### 4.6 Procedure of enquiry/complaint

A Data Subject may contact the Company's Compliance Officer at the contact details given below with inquiries or complaints regarding the Company's processing of Personal Data.



## Network Management Policy

Document No. GIPCL/PL/08

Release Date: 23<sup>rd</sup> May 2020

# Network Management Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>



	<h2>Network Management Policy</h2>	Document No. GIPCL/PL/08
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
4.1	Network Security Design .....	5
4.1.1	Requirements.....	5
4.1.2	Defence in Depth .....	5
4.1.3	Network Segregation .....	5
4.1.4	Perimeter Security .....	6
4.1.5	Public Networks .....	6
4.1.6	Wireless Networks .....	6
4.1.7	Physical Security.....	6
4.1.8	Remote Access.....	7
4.1.9	Network Intrusion Detection .....	7
4.2	Network Security Standards .....	7
4.2.1	Network Hardware .....	7
4.2.2	IP Addressing.....	8
4.2.3	Network Protocols.....	8
4.3	Network Security Management.....	8
4.3.1	Roles & Responsibilities .....	8
4.3.2	Logging & Monitoring .....	9
4.3.3	Network Changes .....	9
4.3.4	Network Security Incidents .....	9
5	Conclusion .....	9



# Network Management Policy

Document No. GIPCL/PL/08

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

This policy indicates the principles that have been used in designing and implementing the security of network. There are many different ways of constructing networks and it is important devise a method to structure the network to provide confidentiality, integrity and availability to the organisation.

## 2 Purpose

This document sets out the GIPCL's policy on how it will design, manage and support computer networks. Its intended audience is IT and information security management and support staff who will implement and maintain the organisation's defences.

## 3 Scope

This policy applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to GIPCL systems.

## 4 Policy

The use of networks is an essential part of the day to day business of GIPCL. Networks not only connect many of the components of business processes together internally, but they also link the organisation with its suppliers, customers, stakeholders and the outside world.

The organisation's networks have evolved over a period of time to become the circulatory system of the company, transporting information to where it needs to go and enabling business to be carried out effectively.

But the fact that so much information runs through our networks makes them a target for those who would try to steal that information and disrupt our business. Therefore these networks need to be protected to ensure that the confidentiality, integrity and availability of our vital information is assured at all times.

The effective protection of our networks requires that we adopt good practices in information security covering the design, implementation, operation and management of them and that we ensure that everyone involved follows these practices.

This policy sets out GIPCL's rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure.



## 4.1 Network Security Design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on a specific set of requirements that are established early on in the process. This policy does not attempt to specify how individual networks should be designed and built, but provides guidance for the standard building blocks that should be used

### 4.1.1 Requirements

A network design should be based on a clear definition of requirements which should include the following security-related factors:

- The classification of the information to be carried across the network and accessed through it
- A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities
- The level of trust between the different components or organisations that will be connected
- The hours of availability and degree of resilience required from the network
- The geographical spread of the network
- The security controls in place at locations from which the network will be accessed
- Security capabilities of existing computers or devices that will be used for access

Requirements should be documented and agreed before design work starts.

### 4.1.2 Defence in Depth

A “Defence in Depth” approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network. For example network firewalls should be supplemented by host-based software firewalls on servers and clients in order to provide several levels of firewall protection.

At key points in the network a “defence diversity” approach should also be taken so that vulnerabilities are minimised. For example this may involve using firewalls from different vendors in series so that if a vulnerability is exploited in one device, the other will not be subject to it. This may be extended to the use of more than one network virus scanner at the perimeter for the same reason.

### 4.1.3 Network Segregation

The principle should be adopted that a network should consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).



## Network Management Policy

Document No. GIPCL/PL/08

Release Date: 23<sup>rd</sup> May 2020

For a large network this should be achieved using separate domains, particularly where separate organisations' networks are being linked. An appropriate level of trust should be configured at the domain level and domain perimeters should be secured using a firewall where appropriate.

Within networks, Virtual Local Area Networks (VLANs) will be used to segregate organisational units.

### 4.1.4 Perimeter Security

At all perimeters between the internal network and an external network (such as the Internet) effective measures should be put in place to ensure that only authorised network traffic is permitted. This will usually consist of at least one Stateful Inspection firewall and for major links with the Internet an Application (or Application Gateway) firewall should be used. For connections such as broadband at smaller locations a Packet Filtering firewall may suffice, depending on the results of a risk assessment.

Servers that are intended to be accessed from an external, insecure network (such as web servers) should be located in a DeMilitarised Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

### 4.1.5 Public Networks

Where information is to be transferred over a public network such as the Internet, strong encryption via SSL must be used to ensure the confidentiality of the data transmitted.

Servers that will be accessed from devices on the public network will be located in the DMZ of the firewall.

### 4.1.6 Wireless Networks

- Wireless networks should be secured using WPA2 encryption. WEP and WPA should not be used.
- Wireless networks should be treated as insecure even if WPA2 is used as the encryption method and a firewall installed between the wireless network and the main LAN.
- A guest wireless network may be provided for visitors. This should be physically separate from all internal networks (including internal wireless networks) and also secured using a firewall.
- Wireless access points should be configured to not broadcast their SSID and to not allow secure connection using WPS (WiFi Protected Setup) via physical access to the access point itself.
- Wireless access point admin logon passwords should always be changed from the default.

### 4.1.7 Physical Security

	<h1>Network Management Policy</h1>	<p>Document No. GIPCL/PL/08</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	------------------------------------	-------------------------------------------------------------------------------------

Remote network equipment will be housed in secure cabinets which will be locked at all times. Only support staff will have access to the key to each cabinet.

Backbone and centralised network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to which only authorised support staff will have access (with the exception of local facilities staff for reasons of health and safety).

Wireless access points located in public areas should be hidden from view where possible and should be placed in positions where access by the public is difficult e.g. in or near the ceiling. A lockable protective casing should be installed where an access point is located in an unprotected public area e.g. a car park.

#### 4.1.8 Remote Access

Where there is a requirement for remote access to the internal network the following controls will be used:

- A Virtual Private Network (VPN) will be used providing session encryption using SSL
- Two factor authentication at the client where appropriate
- Secure authentication using a RADIUS server
- Network Access Control (NAC) will be used to restrict access to remote clients that do not meet minimum requirements e.g. virus control

Remote access should be granted on an “as required” basis rather than for all users by default.

#### 4.1.9 Network Intrusion Detection

A Network-based Intrusion Detection System (NIDS) should be installed at the network perimeter and at all key points within the network e.g. on critical servers.

For networks with high security requirements an Intrusion Prevention System (IPS) should be considered, although its implementation should be approached with caution to avoid a high degree of false positives with corresponding disruption to service to users.

## 4.2 Network Security Standards

The following standards will be adopted with respect to network configuration and security.

### 4.2.1 Network Hardware

Where possible a single supplier policy will be used for network hardware. An exception will be made where the use of multiple vendor hardware may increase the level of security provided e.g. in a dual network-based firewall configuration.

Network routing will be based on Cisco routers using OSPF. Cisco Gigabit switches will be used as standard for connectivity. Switch ports, including diagnostic ports will be configured to be administratively disabled until required. Hubs will not be used due to their inherent security



# Network Management Policy

Document No. GIPCL/PL/08

Release Date: 23<sup>rd</sup> May 2020

weaknesses.

Cat 6 UTP will be used for network cabling unless specific circumstances (such as excessive interference) preclude its use. The network topography used will be Ethernet according to the IEEE 802.3 family of standards.

## 4.2.2 IP Addressing

IPv4 will be used on internal networks. However new network devices purchased should support IPv6 in preparation for the future.

The internal IP address range used will be 192.168.0.0 - 192.168.254.254. the assignment and use of subnets should be monitored carefully.

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP. Internal DNS servers will be used.

## 4.2.3 Network Protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server should be enabled by default in order to reduce the attack surface. This is especially true for servers within the DMZ of the firewall(s).

## 4.3 Network Security Management

Once networks have been designed and implemented based on a clear set of security requirements, there is an ongoing responsibility to manage and control the secure networking environment to protect the organisation's information in systems and applications. This should be achieved via controls in the following areas.

### 4.3.1 Roles & Responsibilities

Roles and responsibilities for the management and control of networks should be clearly defined. In order to provide effective segregation of duties, the operation of networks is managed separately from the operation of the rest of the infrastructure such as servers and applications.

This segregation of duties is detailed in the following table.

Manager Role	Team	Main Responsibilities
Networks Manager	Network and Communications Management	Design and implementation of new and changed networks Installation and removal of networking equipment Configuration of networking equipment Third line incident management

Network Operations Manager	Network Operations	Network availability monitoring Network intrusion monitoring Second line incident management Configuration backups Patching and updates Setup and management of remote access users
Computer Operations Manager	Computer Operations	Server and application backups Job scheduling Infrastructure monitoring First line incident management

### 4.3.2 Logging & Monitoring

Firewall logs will be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a Network-based Intrusion Detection System should be configured to alert the Network Operations team of this activity.

Network monitoring for availability should be achieved using an appropriate SNMP-based network management tool (such as Nagios, Solar Winds or WhatsUp Gold) and recovery actions automated where possible.

Alerts from the Network Access Control (NAC) system should be addressed immediately to ensure that clients that do not meet minimum security requirements are only allowed access to a quarantined subset of systems on the network.

### 4.3.3 Network Changes

All changes to network devices will be subject to the change management process (see ISMS18005 Change Management Process) and appropriate risk assessment, planning and backout methods put in place.

### 4.3.4 Network Security Incidents

Events which are deemed to be network security incidents should be recorded and managed according to the incident management process (see ISMS22002 Incident Management Process).

Major network outages should be managed via the Major Incident Management Process (see ISMS22003 Major Incident Management Process) which provides for the invocation of aspects of the business continuity plan where appropriate.

## 5 Conclusion

Network security is a cornerstone of [Organisation Name]’s defences against many of the threats with which we are faced. Only by designing effective security into every new system and network



	<h1>Network Management Policy</h1>	Document No. GIPCL/PL/08
		Release Date: 23 <sup>rd</sup> May 2020

from the very beginning can effective control be maintained and risk minimised. Further to this, additional controls must be implemented which ensure that proper segregation of duties is achieved and changes to the network environment happen in a managed way.

Combined with watchful monitoring of the network itself and the tools put in place to manage it, this should ensure that the number and severity of network security incidents is minimised and our exposure from those that do occur is not as great as it otherwise might have been.



## Vulnerability Management Policy

Document No. GIPCL/PL/09

Release Date: 23<sup>rd</sup> May 2020

# Vulnerability Management Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujrat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Vulnerability Management Policy</h2>	Document No. GIPCL/PL/09
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Vulnerability Management Policy

Document No. GIPCL/PL/09

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Purpose .....	4
2	Scope.....	4
3	Policy .....	4
3.1	Technical Vulnerability Management .....	4
3.2	What is Technical Vulnerability Management? .....	5
3.3	Sources of Information .....	6
3.4	Patches and Updates .....	7
3.5	Vulnerability Assessment.....	7
3.6	Hardening .....	8
3.7	Awareness Training.....	8



# Vulnerability Management Policy

Document No. GIPCL/PL/09

Release Date: 23<sup>rd</sup> May 2020

## 1 Purpose

This document sets out the GIPCL's policy on how it will assess and manage technical vulnerabilities within the IT environment. Its intended audience is IT and information security management and support staff who will implement and maintain the organisation's defences.

## 2 Scope

This policy applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to GIPCL systems.

## 3 Policy

### 3.1 Technical Vulnerability Management

Malware is any code or software that may be harmful or destructive to the information processing capabilities of the organisation and is one of the primary tools used by attackers to circumvent security in order to make some kind of gain or to disrupt the normal operation of the business.

It is essential that effective precautions are taken by GIPCL to protect itself against this threat which can come from a number of sources including organised gangs, competitor organisations, politically motivated groups, rogue employees, nation state sponsored "cyber-warfare" units or simply individuals exercising curiosity or testing their skills.

Whatever the source, the result of a successful security breach is that the organisation and its stakeholders are affected, sometimes seriously, and harm is caused.

Malware comes in many forms and is constantly changing as previous attack routes are closed and new ones are found. The most common types of malware found today are:

- Virus
- Trojan
- Worm
- Logic bomb
- Rootkit
- Key logger
- Backdoor

	<h1>Vulnerability Management Policy</h1>	Document No. GIPCL/PL/09 Release Date: 23 <sup>rd</sup> May 2020
-----------------------------------------------------------------------------------	------------------------------------------	---------------------------------------------------------------------

Often these types of malware will be used in combination with each other.

In order for malicious software to carry out its intended purpose it needs to be installed on the target device or computer. There are a number of key ways in which malware infects computers and networks, although new ways are being created all the time.

The most common infection techniques are as follows.

- Phishing
- Websites and Mobile Code
- Removable Media
- Hacking

But in order for these techniques to be used by an attacker, they must take advantage of a **Vulnerability** in our defences.

### 3.2 What is Technical Vulnerability Management?

A vulnerability is defined in NIST Special Publication 800-30 Rev 1 as “an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source.”

The software development process is complicated and its output in the form of software programs is rarely bug free. Most of these bugs simply affect the functionality of the software so that it doesn't work as intended. However, if manipulated in the correct way, some can allow an attacker to gain some form of advantage or access which was not intended by the developer. This type of bug is commonly considered to be a software vulnerability.

These vulnerabilities are constantly being found and corrected via software updates or patches. Unfortunately it is not always the developer or user who discovers these vulnerabilities. When discovered by a potential attacker the vulnerability becomes something to be exploited for gain and kept secret for as long as possible. A newly-discovered vulnerability is often referred to as a “zero day exploit” and is difficult to defend against.

GIPCL's policy with respect to technical vulnerabilities is to be aware of them and to close them where possible, either directly or via other means.



## Vulnerability Management Policy

Document No. GIPCL/PL/09

Release Date: 23<sup>rd</sup> May 2020

### 3.3 Sources of Information

The first step in managing technical vulnerabilities is to become aware of them. Since we are talking about technical vulnerabilities these will of course depend upon the technology employed within the organisation. It is necessary then to gain a full appreciation of the technology components that make up the organisation's infrastructure and their versions (since most technical vulnerabilities are very version-specific).



# Vulnerability Management Policy

Document No. GIPCL/PL/09

Release Date: 23<sup>rd</sup> May 2020

This should include:

- Operating systems e.g. Windows, UNIX, Cisco
- Databases e.g. SQL Server, MySQL
- Web servers e.g. IIS, Apache
- Desktop software e.g. Office, Acrobat
- Web technologies e.g. Flash, Java
- Application software e.g. SAP, Agresso
- Hardware e.g. servers, routers

Information about vulnerabilities with any of the above components is generally available from the vendor who will issue updates and patches to fix those that it becomes aware of.

Where configuration changes are recommended to close off vulnerabilities, these should be actioned through the organisation change management process so that appropriate controls are in place for testing, risks assessment and backout.

## 3.4 Patches and Updates

Patches and updates will typically be issued by software vendors on a regular schedule as cumulative packages. These will be linked to the specific version of software that they relate to and may have dependencies stipulated with other software modules, products or operating systems.

The scheduling of the installation of updates will depend upon a number of factors including:

- The criticality of the systems being updated
- The expected time taken to install the updates (and requirements for service outages to users)
- The degree of risk associated with any vulnerabilities that are closed by the updates
- Co-ordination of the updating of related components of the infrastructure
- Dependencies between updates

An update release plan should be created and maintained to keep track of when various system will be updated, taking into account the factors listed above. The plan must be managed through the change management process. For updates that are low risk and regular, a standard change may be defined within the change management process to allow this to happen without excess administrative overhead

## 3.5 Vulnerability Assessment

In addition to the regular application of vendor-supplied software updates, GIPCL will conduct a vulnerability assessment at least twice a year. The focus of the vulnerability assessment should be guided by the most recent risk assessment.

The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker. These could include known software vulnerabilities that have not been patched, configuration errors that need to be corrected or examples of inadequate security practice that need to be addressed.

The assessment may be carried out in-house, by an external company or a combination of both and as a minimum should cover:





# Vulnerability Management Policy

Document No. GIPCL/PL/09

Release Date: 23<sup>rd</sup> May 2020

- Assessment of the security of all routes into the organisation's internal network from the Internet
- Externally-facing web servers
- Business critical servers on the internal network
- A selection of typical user computers

If resources permit, additional areas should be assessed such as the vulnerability of employees to phishing attacks.

It is not the organisation's policy to attempt to exploit the vulnerabilities found as a matter of course. This type of penetration test may be commissioned as required using external specialist resources as part of a carefully planned exercise performed outside of normal business hours.

## 3.6 Hardening

A further action that should be taken to reduce the number and extent of vulnerabilities within GIPCL systems is the hardening of server and other device configurations. This involves the shutting down of services and protocols that are not needed so that the attack surface is reduced.

These hardening activities should be carried out according to vendors' guidelines and under the control of the change management process.

## 3.7 Awareness Training

As a result of vulnerability assessment it may be necessary to increase efforts in security awareness training for employees and contract staff. This training should explain the nature of vulnerabilities and what can be done to reduce them.



## Risk Management Policy

Document No. GIPCL/PL/10

Release Date: 23<sup>rd</sup> May 2020

# Risk Management Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujrat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Risk Management Policy</h2>	Document No. GIPCL/PL/10
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release

## Table of Contents

1	Purpose.....	4
2	Scope.....	4
3	Risk Assessment & Treatment Process .....	4
3.1	Criteria for performing Information Security Risk Assessments .....	5
3.2	Process Diagram.....	6
3.3	Identification of Risks.....	7
3.3.1	Assets .....	7
3.3.2	Threats.....	7
3.3.3	Vulnerabilities.....	7
3.3.4	Likelihood .....	7
3.3.5	Impact.....	7
3.4	Risk Analysis & Evaluation .....	8
3.4.1	Numerical Classification .....	8
3.4.2	Risk Acceptance Criteria.....	9
3.4.3	Risk Assessment Report .....	9
3.5	Risk Treatment .....	10
3.5.1	Risk Treatment Option.....	10
3.5.2	Risk Treatment Plan .....	11
3.6	Selection of Controls .....	11
3.6.1	Statement of Applicability.....	11
3.7	Management Approval .....	11
3.8	Risk Monitoring and Reporting.....	12
3.9	Regular Review .....	12
3.10	Roles and Responsibilities .....	13
3.10.1	RACI Chart .....	13
3.11	Conclusion .....	13



# Risk Management Policy

Document No. GIPCL/PL/10

Release Date: 23<sup>rd</sup> May 2020

## 1 Purpose

The Risk Assessment and Treatment Process documents how risk assessments will be carried out and the resulting risks treated.

The effective management of information security has always been a priority for GIPCL in order to manage risk and safeguard its reputation in the marketplace.

However, there is still much to be gained by GIPCL and by the [IT Department] in introducing industry-standard good practice processes, not the least of which is the ability to become more proactive in our approach to information security and to gain and maintain a better understanding of our customers' needs and plans.

## 2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GIPCL business or interact with internal networks and business systems, whether owned or leased by GIPCL, the employee, or a third party.

This policy applies to employees, contractors, consultants, temporaries, and other workers at GIPCL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by GIPCL.

## 3 Risk Assessment & Treatment Process

Risk is the happening of an unwanted event, or the non-happening of a wanted event, which affects a business in an adverse way. Risk is realised when:

- the objectives of the business are not achieved
- the assets of the business are not safeguarded from loss
- there is non-compliance with organisation policies and procedures or external legislation and regulation
- the resources of the business are not utilised in an efficient and effective manner
- the confidentiality, integrity and availability of information is not reliable

It is important that GIPCL] has an effective risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them.

It is important also that the process is sufficiently clear so that successive assessments produce consistent, valid and comparable results, even when carried out by different people.



## Risk Management Policy

Document No. GIPCL/PL/10

Release Date: 23<sup>rd</sup> May 2020

### 3.1 Criteria for performing Information Security Risk Assessments

There are a number of circumstances in which an information security risk assessment should be carried out and these will vary in scope. In general these are as follows:

- A comprehensive risk assessment covering all information assets as part of the initial implementation of the Information Security Management System (ISMS)
- Updates to the general risk assessment as part of the management review process - this should identify changes to assets, threats and vulnerabilities and therefore risk levels
- As part of projects that involve significant change to the organisation, the ISMS or its information assets
- As part of the change management process when assessing whether proposed changes should be approved
- On major external change affecting the organisation which may invalidate the conclusions from previous risk assessments e.g. changes to relevant legislation

If there is uncertainty regarding whether a risk assessment is appropriate, the organisation should err on the side of caution and carry one out.



## 3.2 Process Diagram

The process of risk assessment and treatment is shown in the diagram below.

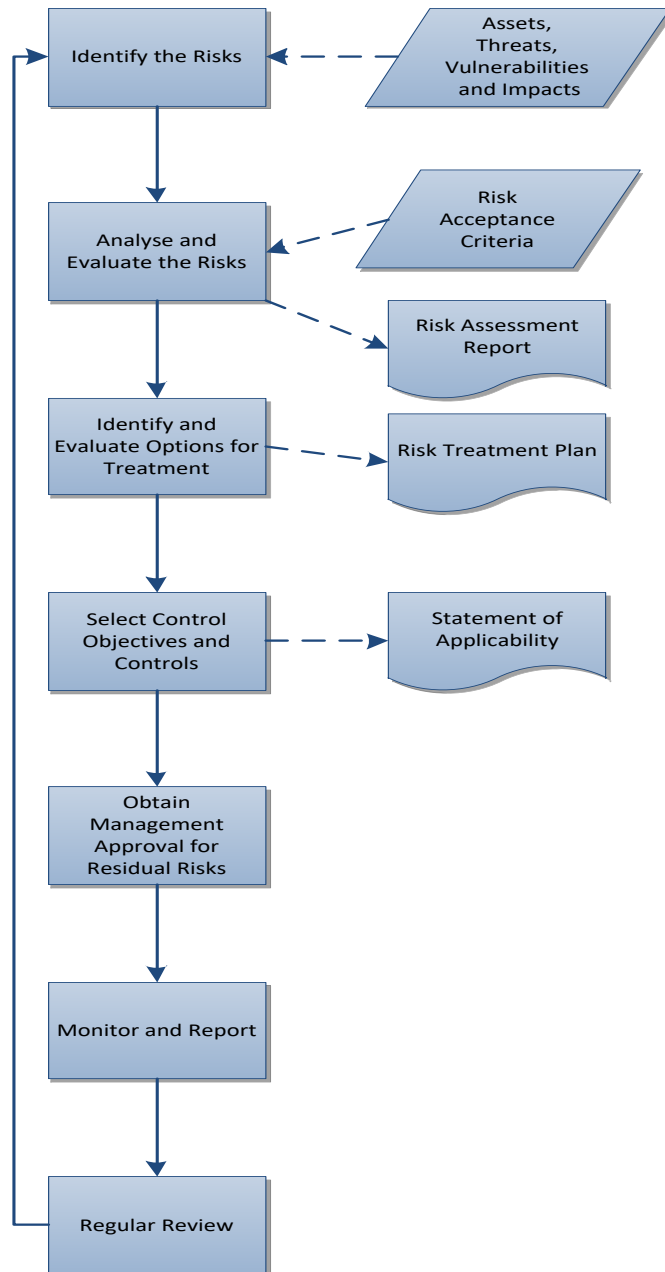


Fig 1 - Risk Assessment and Treatment Process

Each step in this process is described in more detail in the rest of this document.



## 3.3 Identification of Risks

The process of identifying risks will consist of the following steps in line with the requirements of ISO/IEC 27001.

### 3.3.1 Assets

A full inventory of assets will be compiled and maintained by GIPCL. The definition of an asset is taken to be “anything that has value to the organisation” and is therefore worthy of protection. This will include physical assets such as IT servers and operational machinery as well as information assets such as customer lists and application databases.

### 3.3.2 Threats

For each asset, the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft or sabotage. An initial starting list of typical threats is at Appendix A of this document.

### 3.3.3 Vulnerabilities

Circumstances or attributes of an asset which may be capitalised on by any specific threat will be detailed. Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of malware) or the existence of paper files in a data centre (which could be exploited by the threat of fire).

### 3.3.4 Likelihood

An estimate of the likelihood of the threat occurring must be made. This should take into account whether it has happened before either to this organisation or similar organisations in the same industry or location and whether there exists sufficient motive, opportunity and capability for the threat to become real.

### 3.3.5 Impact

Finally an estimate of the impact that the loss of confidentiality, integrity or availability of the asset could have on the organisation should be given.

Consideration should be given to the impact in the following areas:

- Customers
- Finance
- Health and Safety



- Reputation
- Knock-on impact within the organisation
- Legal, contractual or organisational obligations

### 3.4 Risk Analysis & Evaluation

#### 3.4.1 Numerical Classification

To assess the risk to an asset and determine the appropriate treatment, GIPCL will examine the threats, vulnerabilities, the likelihood that the threat will take place and the impact of it should it occur. A 5-point scale will be used to describe the likelihood of a risk taking place and also to describe the impact that it is likely to have.

The 5-point scale for the likelihood ranges from 1=improbable to 5=almost certain; the 5-point scale for the impact ranges from 1=negligible to 5=very high. The risk matrix shown below illustrates the scales and allows us to prioritise our risks so that they can be managed more effectively.

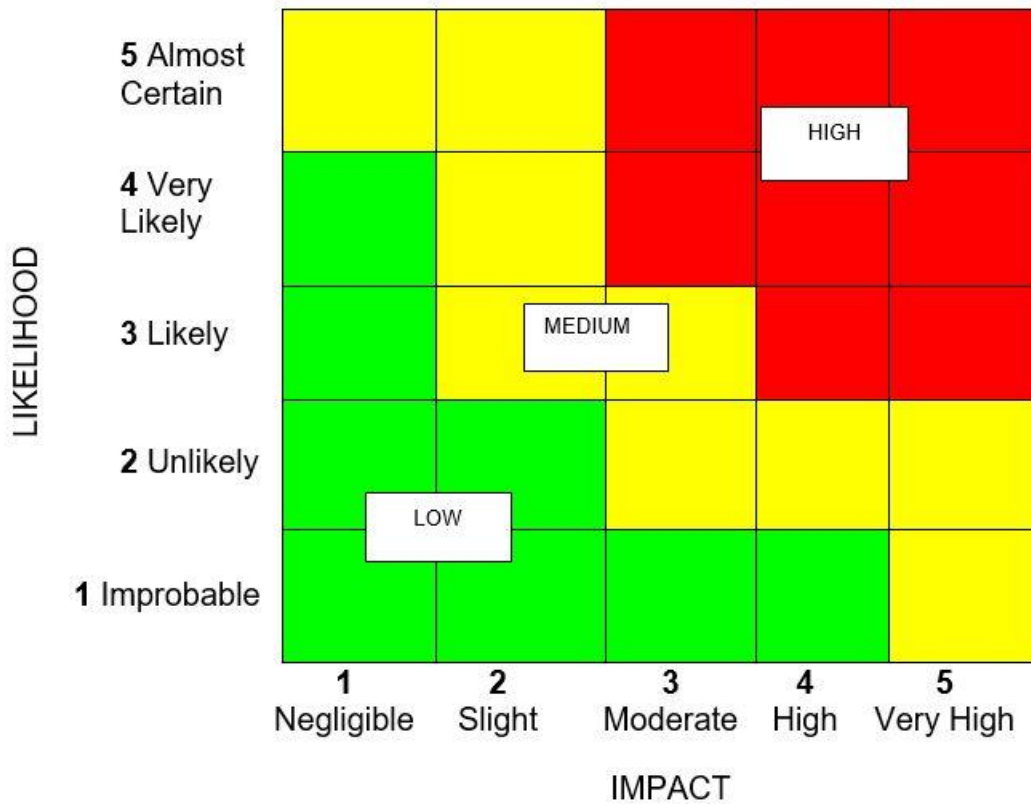


Fig 2 - Risk Matrix Chart

	<h2 style="margin: 0;">Risk Management Policy</h2>	<p>Document No. GIPCL/PL/10</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	----------------------------------------------------	-------------------------------------------------------------------------------------

The risk classification used will be the score obtained from multiplying the likelihood that the risk will occur and the impact it is likely to have. Both scales range from 1 to 5, so the minimum score will be 1 and the maximum score will be 25 as shown in the matrix above.

Each risk will be allocated a classification based on its score as follows:

- HIGH - 12 or more
- MEDIUM - 5 to 10 inclusive
- LOW - 1 to 4 inclusive

The rationale for indicating the likelihood and impact ratings awarded will be given so that these can be assessed at a later date to see if they have materially changed. This will also assist in ensuring consistency and repeatability in risk assessments.

### 3.4.2 Risk Acceptance Criteria

The matrix in Figure 2 shows the classifications of risk, where green indicates an acceptable threshold as the likelihood is minimal or/and the impact is minimal. The yellow indicates that the risk threshold is medium as the risk is larger as is the impact; so containing those risks is more important than addressing those in the green. The red area indicates the risks that are of the highest priority as both the impact and the risk are relatively high, so measures to contain them must be of the highest priority and, if they cannot be reduced then countermeasures must be in place for these risks.

The overall intention of the risk assessment and proposed treatments is to reduce the classification of the risks to an acceptable level e.g. HIGH down to MEDIUM or MEDIUM down to LOW. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g. reducing the score from 8 to 6 means it still remains a MEDIUM level risk. The organisation may decide to accept these risks even though they remain at a MEDIUM rating.

The priorities of the items in the Continual Improvement Plan are determined by the highest priority of the Risk Assessment items addressed e.g. if 3 items are addressed by a single action and one is MEDIUM and two LOW, then the priority of the action will be MEDIUM.

### 3.4.3 Risk Assessment Report

The output from the Risk Analysis and Evaluation stage is the Risk Assessment Report. This shows the following information:

	<h1>Risk Management Policy</h1>	<p>Document No. GIPCL/PL/10</p> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	---------------------------------	-------------------------------------------------------------------------------

- Assets
- Threats
- Vulnerabilities
- Controls currently implemented
- Likelihood (including rationale)
- Impact (including rationale)
- Score
- Classification
- Risk Owner
- Whether the risk is accepted or needs treatment

This report is input to the Risk Treatment stage of the process and must be signed off by management before continuing.

## 3.5 Risk Treatment

For those risks that are judged to be above the threshold for acceptance by GIPCL, the options for treatment will then be explored.

### 3.5.1 Risk Treatment Option

The following options may be applied to the treatment of the identified unacceptable risks:

1. Apply appropriate controls to lessen the likelihood and/or impact of the risk
2. Avoid the risk by taking action that means it no longer applies
3. Transfer the risk to another party e.g. insurer or supplier

Judgement will be used in the decision as to which course of action to follow, based on a sound knowledge of the circumstances surrounding the risk e.g.

- Business strategy
- Regulatory and legislative considerations
- Technical issues
- Commercial and contractual issues

The Risk Manager will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted.



# Risk Management Policy

Document No. GIPCL/PL/10

Release Date: 23<sup>rd</sup> May 2020

## 3.5.2 Risk Treatment Plan

The evaluation of the treatment options will result in the production of the Risk Treatment Plan which will detail:

- Risks above the acceptance threshold
- Assets affected
- Recommended treatment option
- Control Requirements

This document will be input to the next stage in the process where controls will be selected to meet the identified requirements.

## 3.6 Selection of Controls

In accordance with GIPCL's adoption of the ISO/IEC 27001 standard, Annex A of that document will be used as the starting point for the identification of appropriate controls to address the risk treatment requirements identified as part of the risk assessment exercise.

In the event that the controls set out in Annex A do not address all requirements then additional controls may be implemented.

### 3.6.1 Statement of Applicability

The Statement of Applicability will set out those controls from Annex A of the ISO/IEC 27001 standard that have been selected and the reasons for their selection. It will also detail those that have been implemented and identify any that have been explicitly excluded together with a reason for such exclusion.

## 3.7 Management Approval

At each stage of the risk assessment process management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the following documents:

- Risk Assessment Report
- Risk Treatment Plan
- Statement of Applicability

Signoff will be indicated according to GIPCL documentation standards.

	<h1>Risk Management Policy</h1>	Document No. GIPCL/PL/10 Release Date: 23 <sup>rd</sup> May 2020
-----------------------------------------------------------------------------------	---------------------------------	---------------------------------------------------------------------

In addition to overall management approval, each treatment should be signed off by the relevant risk owner.

### 3.8 Risk Monitoring and Reporting

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exception situations can be identified and dealt with by management.

### 3.9 Regular Review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business such as office moves, mergers and acquisitions or introduction of new or changed IT services.



## Risk Management Policy

Document No. GIPCL/PL/10

Release Date: 23<sup>rd</sup> May 2020

### 3.10 Roles and Responsibilities

Within the process of risk assessment there are a number of key roles that play a part in ensuring that all risks are identified, addressed and managed. These roles are shown in the RACI table below, together with their relative responsibilities at each stage of the process.

#### 3.10.1 RACI Chart

The table below clarifies the responsibilities at each step using the RACI model, i.e.:

**R= Responsible      A= Accountable      C= Consulted I= Informed**

Role:	Information Security Manager	Business Management	Operational Staff
Step			
Identify the risks	A/R	C	C
Risk Acceptance Criteria	C	A/R	C
Analyse and Evaluate the risks	A/R	C	C
Identify and Evaluate Options for Treatment	A/R	C	C
Select Control Objectives and Controls	A/R	C	C
Obtain Management Approval for Residual Risks	A	R	C
Monitor and Report	A/R	I	C
Regular Review	A/R	C	C

### 3.11 Conclusion

The process of risk assessment and treatment is fundamental to the implementation of a successful Information Security Management System (ISMS) and forms a significant part of the ISO/IEC 27001 standard.

By following this process GIPCL will go some way to ensuring that the risks that it faces in the day to day operation of its business are effectively managed and controlled.



## Asset Management Policy

Document No. GIPCL/PL/11

Release Date: 23<sup>rd</sup> May 2020

# Asset Management Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujrat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Asset Management Policy</h2>	Document No. GIPCL/PL/11
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release





# Asset Management Policy

Document No. GIPCL/PL/11

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Purpose .....	4
2	Scope.....	4
3	Policy .....	4
3.1	Asset Identification & Classification.....	4
3.2	Classification of Information Assets .....	4
3.3	Labelling of Physical Assets .....	6
3.4	Labelling of Documents .....	6
3.5	Handling of Information Assets.....	6



# Asset Management Policy

Document No. GIPCL/PL/11

Release Date: 23<sup>rd</sup> May 2020

## 1 Purpose

The purpose of this policy is to enable the classification of information assets, the device in which the information resides assets according to varying degrees of sensitivity and criticality. Classification is done on the criticality of the asset depending upon its impact to indicate the need, priorities and expected degree of protection when handling asset. Non-availability of assets of the asset will cause serious or significant consequences to business operation and legal position. All the "assets" referred in the document refers to information Asset.

## 2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GIPCL business or interact with internal networks and business systems, whether owned or leased by GIPCL, the employee, or a third party.

This policy applies to employees, contractors, consultants, temporaries, and other workers at GIPCL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by GIPCL.

## 3 Policy

### 3.1 Asset Identification & Classification

Identification and Classification of information assets is done on the basis of the business needs and the impact of asset loss on the continuity of business. The asset owner identifies the assets in his department in various categories like information, software, physical, etc.

### 3.2 Classification of Information Assets

Information Assets - All information assets (soft/hard copy) are classified based on their confidentiality value ('C' of CIA value) as:

- Confidential
- Privileged and Confidential
- Restricted
- Internal
- Public

**Confidential:** Information is available only to the asset owner, Head of department and senior management. All assets having confidentiality value 5 are classified as Confidential. Only the asset



## Asset Management Policy

Document No. GIPCL/PL/11

Release Date: 23<sup>rd</sup> May 2020

owner can modify these assets.

**Privileged and Confidential:** Information is available only to the asset owner, Head of department, senior management and third party as designated by the asset owner. All assets having confidentiality value 4 are classified as Privileged and Confidential. Only the asset owner can modify these assets.

**Restricted:** Information is available only to the asset owner, Head of department and closed user group for e.g. Operation Teams, Functions and Support Teams. All assets having confidentiality value 3 are classified as Restricted. Only the asset owner or restricted groups/users as mentioned above can modify these assets.

**Internal:** Information is available within the organization or within the asset owner's team/group/department/ team. All assets having confidentiality value 2 are classified as Internal. These assets can be made available to others if authorized by the asset owner. Only the asset owner or a person authorized or designated by him/her can modify these assets.

**Public:** Information is available to the entire organization and to outside parties. All assets having confidentiality value 1 are classified as Public. Only the asset owner or a person authorized or designated by him / her can modify these assets.

In addition to the Asset owner, the respective Head of Department also has the right to change an asset for all above categories. For ZO/PO, the respective Zonal Manager or Chief Project Manager or Head of the office is treated as Head of Department.

	Senior management	HOD's	Asset Owner	Third Parties	Support Team
Confidential	YES	YES	YES	NO	NO
Confidential And Privileged	YES	YES	YES	YES	NO
Restricted	NO	YES	YES	NO	NO
Internal	YES	YES	YES	NO	YES
Public	YES	YES	YES	YES	YES



# Asset Management Policy

Document No. GIPCL/PL/11

Release Date: 23<sup>rd</sup> May 2020

## 3.3 Labelling of Physical Assets

All Physical assets are identified by their allotted Asset code / Asset Serial No. and the allotment of the asset is done through inventory records. Nomenclature of assigning asset code.

It is desirable that assets which are deployed at DC DR will be labelled by the following. Nomenclature of assigning asset code. Asset code / Asset Serial No. /Label. It is desirable that this nomenclature is followed for all Assets.

## 3.4 Labelling of Documents

Physical labels, clearly indicating the classification as Confidential will be affixed on the documents by the originator of the document.

In case of electronic documents, headers/footers are to be added to clearly indicate the labelling as “Privileged and confidential / Confidential / Restricted”.

## 3.5 Handling of Information Assets

Internal & Public documents need not be labelled

	Privileged and Confidential	Confidential	Restricted	Internal
Copying	Copies to be accounted for in the Asset Register.	Copies should be restricted.	Copies should be restricted.	Copies should be restricted.
Storage	Access should only be with the owner, senior management and authorized user or third party as designated by the owner / IT division. Backup copies to be maintained offsite.	Access should only be with the owner, senior management and authorized user / third party designated by the owner / IT division. Backup copies to be maintained offsite.	Access should only be with the asset owner and closed user group and authorized user / third party designated by the owner / IT division. Backup copies to be maintained offsite.	Read access to the whole organization. Backup copies to be maintained offsite.
Transmission	Can be sent through email / post / courier. Security should be ensured in case of courier	Can be sent through email / post / courier / fax. Security should be ensured in case	Can be sent through email / post / courier / fax. Security should be ensured in case of courier	Can be sent through mail / post / courier / fax.

	<h2>Asset Management Policy</h2>	Document No. GIPCL/PL/11
		Release Date: 23 <sup>rd</sup> May 2020

		of courier		
Destruction	Any copies not in use should be destroyed securely.	Any copies not in use should be destroyed securely	Any copies not in use should be destroyed securely.	Any copies not in use should be destroyed securely.

**On violations of this policy, Management may take appropriate disciplinary action.**



## Clean Desk Clear Screen Policy

Document No. GIPCL/PL/12

Release Date: 23<sup>rd</sup> May 2020

# Clean Desk Clear Screen Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013


Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujarat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Clean Desk Clear Screen Policy</h2>	Document No. GIPCL/PL/12
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Clean Desk Clear Screen Policy

Document No. GIPCL/PL/12

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4





# Clean Desk Clear Screen Policy

Document No. GIPCL/PL/12

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

A clean desk and clear screen policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

## 2 Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk and clear screen" - where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site.

## 3 Scope

This policy applies to all GIPCL employees and affiliates.

## 4 Policy

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when unattended this can be achieved by CTRL+ALT+DEL or enforcing password protected screen saver with automatic timeout.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.



## Clean Desk Clear Screen Policy

Document No. GIPCL/PL/12

Release Date: 23<sup>rd</sup> May 2020

- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.
- Computer or laptop screen should always be clear so that sensitive data is not displayed on the main screen,
- All the important files on laptops and desktop should be kept inside the drives.
- Backup of all important files and folders should be regularly taken.

**On violations of this policy, management may take appropriate disciplinary action.**



## Organisation Structure

Document No. GIPCL/PL/13

Release Date: 23<sup>rd</sup> May 2020

# Organisation Structure



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Organisation Structure</h2>	Document No. GIPCL/PL/13
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



# Organisation Structure

Document No. GIPCL/PL/13

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Policy.....	4
4.	Roles and Responsibility.....	4
4.1	Information Security Management Forum (ISMF) - Chairman .....	5
4.2	Information Security Team.....	6
4.3	Chief Information Security Officer (CISO).....	6
4.4	Information Security Officers (ISOs).....	6
4.5	Information Users and Risk Owner .....	7



# Organisation Structure

Document No. GIPCL/PL/13

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This document also outlines the implementation of structural changes including special placement and selection measures for realignments of organizational units and the sub-processes involved in post design, classification and reclassification.

## 2 Purpose

The purpose of organizational structuring is to further the mandate of the organization by ensuring that it is able to meet organizational needs and efficiently uses its resources.

## 3 Policy

### General guideline

The policy outlines the conditions and procedures for structuring organizational units and identifies control actions to mitigate potential risks related to the process as summarised below:

1. Heads of unit must obtain approval from the Deputy Executive Director (Programme) (DED-P) for offices in the field, and Deputy Executive Director (Management) (DED-M) for HQ and offices under the Office of the Executive Director, and endorsement from their relevant director, to initiate the process of organizational structuring in cases in which this process is not initiated directly by the Executive Director.
2. Normally organizational structuring will be carried out in conjunction with the country or regional programme, budget process, or changes in funding. Examples of drivers that may result in the need to create or restructure an organizational unit are provided in the following section: Procedures.
3. Any unit requesting organizational structuring must use the standardized documents,
4. An organizational structuring proposal must be cleared by the head of unit and endorsed by the relevant director. The Division for Human Resources will initiate the clearance process and ensure all offices that need to be involved are consulted.

## 4. Roles and Responsibility

### ESTABLISHING OR RESTRUCTURING ORGANIZATIONAL UNITS

The organization needs an optimal design for the organization as a whole, for each organizational unit, and for every individual post. Organizational changes can result in the need to modify the

	<h2>Organisation Structure</h2>	Document No. GIPCL/PL/13
		Release Date: 23 <sup>rd</sup> May 2020

organizational structure by establishing or restructuring an organizational unit, or by changing some individual posts.

**organizational unit could include, but are not limited to:**

- Changing programme requirements
- Expiration of finite mandates (such as programme cycles or technical assistance programmes)
- New country programme cycles and priorities
- Post conflict or emergency situations
- Changes in budget and funding
- Audit findings or the outcome of investigation

#### 4.1 Information Security Management Forum (ISMF) - Chairman

The ISMF (Steering Committee) is responsible for the establishment, implementation, operation, monitoring, review, maintenance and improvement of the security program.

The responsibilities of the ISMF Chairman

- a) Ensure that security objectives and plans for Organisation are established;
- b) Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
- c) Providing sufficient resources to develop, implement, operate and maintain the security program.
- d) Identifying the acceptable levels of risk.
- e) Implementing the new or modifying the information security policies and procedures.
- f) Ensuring that an internal audit is carried out annually and a third-party audit based on requirement.
- g) Ensuring relevant training and, if necessary, employing competent personnel to satisfy the security requirements of Organisation.
- h) The **authorities** of the ISMF Chairman
- i) Reviewing the status of the Organisation -ISACC Services security once in a year. b) Risk Owners approve the residual risk in consent with ISM Chairman.
- j) Approving new or modified information security policies and procedures.
- k) Approving major initiatives in enhancing Information security.

	<h2>Organisation Structure</h2>	Document No. GIPCL/PL/13
		Release Date: 23 <sup>rd</sup> May 2020

The ISMF shall meet quarterly to discuss and review the security program. This meeting shall be chaired by the ISMF, Chairman.

### 4.2 Information Security Team

Information Security Team will comprise the CISO and ISOs for creation, maintenance and monitoring of the ISMS. This team will coordinate with ISMF chairmen through the CISO. The roles and responsibilities of IST (CISO, ISO & Implementation Team) are given below:

### 4.3 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is responsible for the following:

1. ISACC Services representative with respect to inquiries from Organisation -ISACC Services Customers, regarding the organization's security strategy.
2. Implementing the new or modifying the information security policies and procedures.
3. ISACC Services representative when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees or other external entities.
4. Balance security needs with Organisation strategic business plan, identify risk factors, and determine solutions to both.
5. Develop security policies and procedures that provide adequate business application protection without interfering with core business requirements.
6. Oversee the selection testing, deployment, and maintenance of security hardware and software products as well as outsourced arrangements.
7. Oversee a staff of employees responsible for ranging from network technicians to security guards.

### 4.4 Information Security Officers (ISOs)

The ISOs are appointed by ISMF Chairman and are responsible for acting as information systems security coordinators.

- a) ISOs serve as local information security liaisons, implementing the requirements of the security policies and procedures.



	<h2>Organisation Structure</h2>	Document No. GIPCL/PL/13
		Release Date: 23 <sup>rd</sup> May 2020

- b) ISOs are responsible for ensuring that appropriate Organisation measures are observed in their respective business function area.
- c) ISOs shall ensure all users are aware of Organisation policies

**Reporting:** IS Officer will report to the CISO.

#### 4.5 Information Users and Risk Owner

**Risk owners** are responsible for classifying and labelling their information assets and adopting appropriate mechanisms for securing them. This classification and labelling shall comply with the ISO 27001:2013 prescribed controls.

##### **Responsibilities:**

- a) Manage the organization, accuracy and integrity requirements of data.
- b) Identify data that requires restricted access.
- c) Define data access authorization privileges for their Information.
- d) Define security requirements to be built into the operating environment.
- e) Define records retention and destruction schedules for their data which comply with operational, legal and regulatory requirements.
- f) Communicate the “Information protection” requirements to the IT Team.

##### **Authorities:**

- a) Review and approve requisition for changes.
- b) Acceptance of the residual information security risks
- c) Approval of Information Security Risk Treatment Plan in consent with ISMF Chairman.

**Information Users** are responsible for complying with all relevant operational procedures and Information Security Policy defining assigned tasks and relevant Information security measures.

##### **Responsibilities:**

- a) Protect the information and data they are handling.
- b) Be accountable for the effective implementation of controls and protective measures for information assets.
- c) Identify security incidents and weakness.
- d) Provide effective feedback for taking corrective actions.

**On violations of this policy, management may take appropriate disciplinary action.**



## Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

# Acceptable Use Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Acceptable Use Policy</h2>	Document No. GIPCL/PL/14
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	5
4.1	General Use and Ownership .....	5
4.2	Security and Proprietary Information .....	5
4.3	Unacceptable Use.....	6



# Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

GIPCL ISMS's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to GIPCL philosophy, but to establish a culture of openness, trust and integrity. GIPCL ISMS is committed to protect GIPCL employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Apart from that, it intends to bring standardization as it is most important part of running any organization.

Internet/intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of GIPCL. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every GIPCL employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment's at GIPCL. These rules are in place to protect the GIPCL employees. Inappropriate use exposes GIPCL to information security risks including virus attacks, compromise of network systems and services, and legal issues.

## 3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GIPCL business or interact with internal networks and business systems, whether owned or leased by GIPCL, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at GIPCL are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with GIPCL policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at GIPCL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by GIPCL.



# Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

## 4 Policy

### 4.1 General Use and Ownership

- GIPCL's proprietary information stored on electronic and computing devices whether owned or leased by GIPCL, the employee or a third party, remain the sole property of GIPCL. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of GIPCL proprietary information.
- You may access, use or share GIPCL proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within GIPCL may monitor equipment, systems and network traffic at any time.
- GIPCL reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 4.2 Security and Proprietary Information

- All IT related peripherals and computing devices that connect to the internal network must comply with the Minimum Access Policy, means device must be in domain OR registered with GIPCL ISMS.
- System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screen saver with the automatic activation feature set to 10 minutes or less or you must lock the screen or log off when the device is unattended.



## Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

- Postings by employees from a GIPCL email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of GIPCL, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### 4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of GIPCL is authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing GIPCL owned resources.

The list below is by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

#### Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by GIPCL.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which GIPCL or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting GIPCL's business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This



## Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

includes family and other household members when work is being done at home.

- Making fraudulent offers of products, items, or services originating from any GIPCL account.
- Using GIPCL's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to GIPCL ISMS is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honey pots, honey nets, or similar technology on the GIPCL network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, GIPCL employees to parties outside GIPCL.
- Stored the non-business data in the desktop PC like Porn photo/Movie, movie, any criminal materials, any harmful data or program.

### Email and Communication Activities

- When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).





## Acceptable Use Policy

Document No. GIPCL/PL/14

Release Date: 23<sup>rd</sup> May 2020

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within GIPCL networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by GIPCL or connected via GIPCL network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### **Blogging and Social Media**

- Blogging by employees, whether using GIPCL property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of GIPCLs' systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate GIPCLs' policy, is not detrimental to GIPCLs' best interests, and does not interfere with an employee's regular work duties. Blogging from GIPCL systems is also subject to monitoring.
- GIPCLs' Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of GIPCL and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by GIPCL.
- Employees may also not attribute personal statements, opinions or beliefs to GIPCL when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of GIPCL. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, GIPCLs' trademarks, logos and any other GIPCL intellectual property may also not be used in connection with any blogging activity.

	<h2>Acceptable Use Policy</h2>	Document No. GIPCL/PL/14 Release Date: 23 <sup>rd</sup> May 2020
-----------------------------------------------------------------------------------	--------------------------------	---------------------------------------------------------------------

**On violations of this policy, management may take appropriate disciplinary action.**



## Fire Safety Plan and Evacuation Policy

Document No. GIPCL/PL/15

Release Date: 23<sup>rd</sup> May 2020

# Fire Safety Plan and Evacuation Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Fire Safety Plan and Evacuation Policy</h2>	Document No. GIPCL/PL/15
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



## Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Procedure .....	4
4	Fire Evacuation Strategy .....	4
4.1	Simultaneous Evacuation .....	4
4.2	Action on hearing the Fire alarm .....	5
4.3	Identification of key escape routes .....	5
4.4	Fire Wardens/Marshals.....	5
5	Fire alarms and drills .....	5



# Fire Safety Plan and Evacuation Policy

Document No. GIPCL/PL/15

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This plan applies to all occupants of organization which are working in an organization Infrastructure

## 2 Purpose

The purpose of this plan is to establish procedures and duties, to promote planning, and to establish training for the staff in case of fire.

## 3 Procedure

**Fire evacuation Plans shall include the following:**

1. Emergency or escape routes and evacuation of the building is to be complete or, where approved, by selected floors or areas only.
2. Employees who must operate critical equipment is should be in procedure before evacuating.
3. Procedures for accounting for employees and occupants after evacuation have been completed.
4. Identification and Assignment of personnel responsible for rescue or emergency medical facilities.

## 4 Fire Evacuation Strategy

It includes the action to be taken by all staff in the event of **fire** and the arrangements for calling the **fire** brigade.

### 4.1 Simultaneous Evacuation

The evacuation in case of fire will simply be by means of everyone reacting to the warning signal given when a fire is discovered, then making their way, by the means of escape, to a place of safety away from the premises This is known as a simultaneous evacuation. And its initiated by the Sounding of the general alarm over the fire warning system.



## Fire Safety Plan and Evacuation Policy

Document No. GIPCL/PL/15

Release Date: 23<sup>rd</sup> May 2020

### 4.2 Action on hearing the Fire alarm

The Fire Marshal(s) should instruct all personnel upon hearing the fire alarm to act in accordance with the agreed strategy.

### 4.3 Identification of key escape routes

In premises where members of the public or persons unfamiliar with layout of the premises are present there should be means available to identify the key escape routes. They could include schematic drawings supplemented with a satisfactory emergency escape signs.

### 4.4 Fire Wardens/Marshals

The Responsible Person where necessary to safeguard the safety of employees should nominate employees to implement certain fire safety measures which will include the fire evacuation. The general term used for these people are fire wardens or fire marshals.

## 5 Fire alarms and drills

1. Held at regular intervals
2. Records kept
3. There should be drills completed at least once a year, from sounding of alarm to roll call procedure
4. Fire Alarms and Fire Fighting Equipment should be tested at weekly intervals and records kept
5. Fire equipment regularly serviced

**On violations of this policy, management may take appropriate disciplinary action.**



## System Security Policy

Document No. GIPCL/PL/16

Release Date: 23<sup>rd</sup> May 2020

# System Security Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>



	<h2 style="margin: 0;">System Security Policy</h2>	Document No. GIPCL/PL/16
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# System Security Policy

Document No. GIPCL/PL/16

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Policy.....	4
4	Personal Responsibilities.....	4
5	Office Procedure .....	5
6	Encrypted Devices.....	5
7	Secure Remote Access.....	5
8	Asset Management .....	5
9	Password Management .....	5
11	Incident Reporting.....	5
11	Training .....	6
12	Policy Review & Further Guidance.....	6



# System Security Policy

Document No. GIPCL/PL/16

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This policy covers all technical implementations and security of local or remote access and also devices used includes Laptop, Computer and other Devices is used in the Organization.

## 2 Purpose

The Purpose of this Policy, the term 'Device' includes, but is not restricted to, laptops, computer and devices which can used to access, Store, Process, Transmit, discuss, or record data electronically.

## 3 Policy

### General guideline

#### SECURITY PROCEDURES FOR STAFF USING LAPTOPS

The user is required to sign the declaration issued by IT Assist accepting that they will comply with the security procedures and acknowledging that they are responsible for the physical security of the laptop as well as the information stored on them.

## 4 Personal Responsibilities

1. Users are responsible for the physical security of their laptop and Computer at all times.
2. Laptops and Desktop must always be carefully looked after to minimise the possibility of loss or theft, unauthorized use, or tampering.
3. Laptops and Desktop must not be left in an unattended car or in an unsecured area.
4. When using the laptop outside a formal secure area, consideration must be given to the possibility of eavesdropping or snooping. Staff must only use the laptop when it is safe to do so, particularly when entering passwords and should be mindful of the risk posed by cameras. In public areas the threat of theft should also be considered.
5. The laptop and Desktop remain the property of IT Assist and must only be used for official purposes.
6. Employees must ensure that their laptop is not used by anyone else.
7. Laptops for training purposes are allocated to an individual member of organization who is responsible for ensuring that appropriate security controls are in place for the security and management.

	<h1>System Security Policy</h1>	Document No. GIPCL/PL/16
		Release Date: 23 <sup>rd</sup> May 2020

## 5 Office Procedure

Laptops must be properly closed down at the end of the day (i.e. selecting shutdown from the operating system menu) and secured in a suitable locked cabinet<sup>2</sup> within the place of work.

## 6 Encrypted Devices

1. External media products officially approved for use can be connected to the laptop.
2. Personal or sensitive data must use encryption and all other data must use encryption.

## 7 Secure Remote Access

1. For Secure Remote Access, users **MUST** only use Internet Explorer to ensure compliance with the internet access security policy.
2. The IT Assist Helpdesk must also be contacted to request a PIN change or report the Loss

## 8 Asset Management

1. Any breach of this policy will be viewed as a security incident and dealt with as such, possibly leading to disciplinary action.
2. All devices must be recorded on the Assets Register.

## 9 Password Management

1. Users must not share passwords/PINs with others.
2. If you suspect that your password/PIN has been compromised you must report this to the Organisation.

## 10 Incident Reporting

All Incident or Breaches of Security Must be Reported Immediately or as soon as reasonably possible to IT Assist.

1. Users should keep a record of the laptop Badge Number and contact information needed in an emergency to report if the laptop is lost or stolen.
2. Users should attempt to power down and secure the laptop if they have any warning that it is likely to be maliciously taken from them.

	<h2>System Security Policy</h2>	Document No. GIPCL/PL/16
		Release Date: 23 <sup>rd</sup> May 2020

3. Damage to (including suspected tampering) or loss of a laptop, other device must be reported at the earliest opportunity to the Organisation.

### 11 Training

When issued with a laptop, users will be given appropriate instructions on the use of the security functionality and their responsibility for safeguarding the laptop and Desktop.

### 12 Policy Review & Further Guidance

This policy will be reviewed annually or in response to new legislation or regulation or following a significant security incident.

**On violations of this policy, management may take appropriate disciplinary action.**



## Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

# Internet Access Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h1>Internet Access Policy</h1>	Document No. GIPCL/PL/17
		Release Date: 23 <sup>rd</sup> May 2020

## Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview.....	4
2	Purpose .....	4
3	Scope .....	4
4	Policy.....	4
4.1	General Guideline.....	4
4.2	Internet Access .....	5
4.3	Acceptable Use .....	6
4.4	Prohibited Usage .....	6
4.5	Maintaining corporate image .....	8
4.6	Security and Monitoring .....	9
4.7	Compliance.....	9





# Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

## 2 Purpose

The purpose of this policy is to define the appropriate uses of the Internet by GIPCL employees and affiliates.

## 3 Scope

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

This policy applies to all users with access to Internet and related services through the GIPCL network infrastructure like internet link, data card, modems etc. Internet related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (e-mail), File Transfer Protocol (FTP), TELNET, RCP and World Wide Web (WWW) access.

## 4 Policy

### 4.1 General Guideline

➤ The users of GIPCL network infrastructure should be aware that several network usage issues are covered by the Indian IT Act 2000 and Indian IT Act 2008, violation of which is an offence



# Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

under national law.

➤ It is understood and presumed by the management of GIPCL that the users are made aware of the contents of this policy document as part of their induction process and users agree to abide by its provisions. Existing users will be informed about the internet usage policy through email.

## 4.2 Internet Access

Based on functional requirements and recommendation of CA, internet access has been provided to existing internet users as per following access groups. Any changes in existing access will require approval of concerned HoM.

Sr	Group Name	Access Hours	Bandwidth Allowed on	
			Primary Line	Backup Line
1	1 Hour Group	1 Hour	1 Mbps Restricted	256 Kbps Restricted
2	2 hour Group	2 Hours	1 Mbps Restricted	256 Kbps Restricted
3	3 Hour group	3 Hours	1 Mbps Restricted	256 Kbps Restricted
4	4 Hour Group	4 Hours	1 Mbps Restricted	256 Kbps Restricted
5	ADM	Office Hours	1 Mbps Restricted	256 Kbps Restricted
6	IT Slpp	24 Hours	1 Mbps Restricted	No Access
7	Open	24 Hours	No Restriction	No Restriction
8	Open Group	24 Hours	1 Mbps Restricted	256 Kbps Restricted
9	Secretarial	24 Hours	1 Mbps Restricted	256 Kbps Restricted
10	User Specific	24 Hours	No Restriction	256 Kbps Restricted

### 1) New Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy. Access will be granted as per above mentioned table. Exceptional Access will be given based on special functional requirements and approval of HoM.

### 2) Removal of Privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the



# Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

## 4.3 Acceptable Use

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;
- IT technical support for downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory, technical or functional information.
- Research

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

## 4.4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property, Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file



## Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

information, and accessing information that is not needed for the proper execution of job functions.

- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs. Any form of gambling.

Following activities are also strictly prohibited:

- No user must download any software, tools and utilities (freeware, shareware or licensed) from the internet without prior written permission of Corporate IT head.
- Trial version of any software in use must be deleted at the end of the trial period or licenses must be procured.
- Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.
- Access to the internet from company laptop or through company connection (data card, modem etc) must adhere to this policy.
- User must not connect their workstation / laptops to the internet through cellular phones or cellular devices (data card, modem) unless such access and the device has been approved by Corporate IT head.

IT Department shall block access to Internet websites and protocols that are deemed inappropriate



## Internet Access Policy

Document No. GIPCL/PL/17

Release Date: 23<sup>rd</sup> May 2020

for GIPCL corporate environment. The following categories of websites shall be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking tools and pirated material
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- Anti-national and anti-social content
- External proxies
- Trading / e-commerce
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate, terrorism
- Web Based Email and message board

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

### 4.5 Maintaining corporate image

1. When using company resources to access and use the Internet, users must realize that they represent the company. Whenever users state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

	<h1>Internet Access Policy</h1>	<p>Document No. GIPCL/PL/17</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	---------------------------------	-------------------------------------------------------------------------------------

2. Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by respective HOD and will be placed by an authorized individual.

#### 4.6 Security and Monitoring

1. Users should consider that their Internet activities are periodically monitored and limit their activities accordingly. Management reserves the right to examine e-mail, personal file directories, web access and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.
2. Users who identify or perceive an actual or suspected security problem shall immediately contact GIPCL IT team.

#### 4.7 Compliance

1. All terms and conditions as stated in this policy document are applicable to all users of the GIPCL IT network infrastructure.
2. To ensure compliance with this policy, periodic reviews will be conducted.
3. If a user does not understand any part of the policy during the induction process or thereafter, it is their responsibility to obtain clarification from IT Department. On violations of this policy, management may take appropriate disciplinary action.

**On violations of this policy, management may take appropriate disciplinary action.**



## E-Mail Access Policy

Document No. GIPCL/PL/18

Release Date: 23<sup>rd</sup> May 2020

# E-Mail Access Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>E-Mail Access Policy</h2>	Document No. GIPCL/PL/18
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release





# E-Mail Access Policy

Document No. GIPCL/PL/18

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Policy .....	4
4.1	General Guidelines.....	4
4.1	Authorization for Provision / Deletion of E-mail ids .....	5
4.2	Creation of Email id's.....	5
4.3	Deletion of E-mail ids.....	5
4.4	Approved Uses .....	6
4.5	Prohibited Uses .....	6
4.6	E-mail System Backup Responsibility .....	7
4.7	Management Access to E-mail Systems Responsibility .....	7
4.8	Email Etiquettes .....	7
4.9	Storing and Deleting Emails .....	8
4.10	Maintaining Corporate Image .....	9
4.11	Security and Monitoring .....	9
4.12	<b>Compliance</b> .....	10
4.13	Incident Reporting .....	10

	<h1>E-Mail Access Policy</h1>	Document No. GIPCL/PL/18
		Release Date: 23 <sup>rd</sup> May 2020

## 1 Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

## 2 Purpose

The purpose of this email policy is to ensure the proper use of GIPCL email system and make users aware of what GIPCL deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within GIPCL Network.

## 3 Scope

This policy covers appropriate use of any email sent from a GIPCL email address and apply to all employees, vendors and agents operating on behalf of GIPCL.

## 4 Policy

### 4.1 General Guidelines

- 1) The users of GIPCL email and messaging infrastructure should be aware that several network usage issues are covered by the Indian IT Act 2000 and Indian IT Act 2008, violation of which is an offence under national law.
- 2) Users must take care when attaching documents or files to an email. Letters, file and other documents attached to emails may belong to others. By forwarding this information, without permission of from the sender, to another recipient you may be liable for copyright infringement.
- 3) This policy is posted on the Intranet of GIPCL and all users who use GIPCL email and messaging resources should be made aware of this policy during the induction process
- 4) It is understood and presumed by the management of GIPCL that the users are made aware of the contents of this policy document as part of their induction process and agree to abide by its provisions. Existing users would be informed about the email policy through email and on notice boards.

	<h2>E-Mail Access Policy</h2>	<p>Document No. GIPCL/PL/18</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-------------------------------	-------------------------------------------------------------------------------------

### 4.1 Authorization for Provision / Deletion of E-mail ids

The person nominated by HOD IT dept will be responsible for provision/deletion of all ids and effective management of email system. All communication will be marked to him on the subject.

### 4.2 Creation of Email id's

Email ids for internal communication within GIPCL by employee will be routed through their respective HODs for its creation. Email ids for internal use within GIPCL and also for communication with external world will be routed through respective HODs.

### 4.3 Deletion of E-mail ids

Email ids will be deleted by default by system administrator on receipt of intimation as under:

#### Employee Serving in the Company

From HODs in respect of all ids used by employee of their respective department & all ids used by employee for internal and external communication.

#### Employee not Serving in the Company

1. In case of employee retiring/leaving the organization, on receipt of communication from HR Dept.

#### Time for provision/deletion of ids

All type of ids will be provisioned/deleted by System Admin within 03 days after receipt of communication from appropriate authority.

#### Use of email ids

All users will use email ids through Microsoft Outlook which will automatically download mails on their desk top for effective email management and space management of email servers.

#### Allocation of Mail Quota:

All user will be allocated fix quota for storage of mails on server. The broad category and allocated quota size are mentioned below:

	<h2 style="margin: 0;">E-Mail Access Policy</h2>	Document No. GIPCL/PL/18
		Release Date: 23 <sup>rd</sup> May 2020

Sr No.	User Group	Description	Retention period of Mails on Server in years
1	Core	MD, MD Office, HOMs, HOMs Office, Chiefs of following departments: Finance, HRA, Projects, SCM, IT	3
2	Senior Management	AGM and IMC Members	2.5
3	Middle Management	DGM, Chief Managers, Sr. Managers	2
4	Junior Management	Manager, Dy. Manager, Asst. Manager, Officers	1.5
5	Others	All other grades, trainees, contract employees etc	1

Attachment limit will be 35 MB in all cases. In exceptional cases any user needs more attachment for critical cases may approach IT dept through their HODs which can be extended on case to case basis after approval of Corporate IT head.

#### 4.4 Approved Uses

- 1) The company provided e-mail access is intended to be for business use only. All e-mail messages shall be considered as records and there must be no expectation of personal privacy.
- 2) Incidental and occasional personal use of official e-mail system is permitted. However, information and messages stored in these systems shall be treated in the same manner as business-related information and may be archived, monitored, or revealed to relevant authorities (if required).

#### 4.5 Prohibited Uses

Unauthorized use of official e-mail systems includes, but is not limited to:

- 1) Transmitting or storing offensive material
- 2) Compromising the security of information contained on the Emails/ Computers
- 3) Soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user's employment and the user's responsibilities towards GIPCL
- 4) Sending or forwarding chain mails



## E-Mail Access Policy

Document No. GIPCL/PL/18

Release Date: 23<sup>rd</sup> May 2020

- 5) Employees must not use the official e-mail system for sending mails greetings containing graphics to any user external or internal.
- 6) Subscribing to non-work-related mailing lists
- 7) Users must not auto forward their e-mails to any personal e-mail ID.
- 8) The official mail system or e-mail IDs must not be used to send bulk mails to external parties.

### 4.6 E-mail System Backup Responsibility

- 1) E-mail messages residing on the E-Mail server must be backed up at least on a daily basis by IT dept.
- 2) Users must take back up of their downloaded e-mails (PST / NSF file) at least on a monthly basis on to the storage provided by IT dept of respective location. All users must download mail on to their local workstations and clear the online mailbox prior to taking back up.

### 4.7 Management Access to E-mail Systems Responsibility

- 1) The Corporate IT head with approval from the HR Head and Departmental Head may inspect and review any information maintained in the e-mail system without prior consent of, or notification to the user concerned.
- 2) The Corporate IT head with approval from the respective HR and Departmental Heads concerned, may disclose contents of email either internally or to external parties, wherever necessary, for a legal or legitimate business reason, without further permission of the employee, trainee or contract personnel.
- 3) Mail Administrators must not be permitted to access, copy, forward another individual's e-mail without approvals of the Corporate IT head.

### 4.8 Email Etiquettes

- 1) Your colleagues may use commonly accepted abbreviations in e-mail, but when communicating with external customers, everyone should follow standard writing protocol. Your e-mail message reflects you and GIPCL, so traditional spelling, grammar and punctuation rules apply.
- 2) USING ALL CAPITAL LETTERS LOOKS AS IF YOU'RE SHOUTING. Using all lowercase letters looks lazy. For emphasis, use asterisks or bold formatting to emphasize important words. Do not, however, use a lot of colours or graphics embedded in your message, because not everyone uses an e-mail program that can display them.



## E-Mail Access Policy

Document No. GIPCL/PL/18

Release Date: 23<sup>rd</sup> May 2020

- 3) Avoid using BCC to keep others from seeing who you copied; it shows confidence when you directly CC anyone receiving a copy. Do use BCC, however, when sending to a large distribution list, so recipients won't have to see a huge list of names. Be cautious with your use of CC; overuse simply clutters inboxes. Copy only people who are directly involved.
- 4) Send group e-mail only when it's useful to every recipient. Use the "Reply All" button only when compiling results requiring collective input and only if you have something to add.
- 5) Be specific in the Subject line and try and reflect the message in the email body. Don't just say, "Hi!" or "From Me".
- 6) Remember that your tone can't be heard in e-mail. E-mail communication can't convey the nuances of verbal communication. In an attempt to infer tone of voice, some people use emoticons, but use them sparingly so that you don't appear unprofessional. Also, don't assume that using a smiley will diffuse a difficult message.
- 7) To ensure that people know who you are, include a signature that has your contact information, including your mailing address, Web site, and phone numbers. This would be handled automatically by the GIPCL systems when your email account is configured. DO NOT alter the standard company signature. Refer to "Maintaining Corporate Image" later in this document.
- 8) Summarize long discussions. Scrolling through pages of replies to understand a discussion is annoying. Instead of continuing to forward a message string, take a minute to summarize it for your reader. You could even highlight or quote the relevant passage, then include your response.

### 4.9 Storing and Deleting Emails

- 1) If an e-mail that you have sent or received has on-going value, either as a source of information, evidence or accountability, then it should be retained for future reference. Received e-mails which have no lasting value should be deleted as soon as their purpose is complete.
- 2) Outlook users who need to store e-mails outside to the system (e.g. in project/case related folders or workspaces) should store e-mails in Outlook Message Format (\*.msg). This ensures that the complete background information ("metadata") is retained, such as the date and time of transmission and the server routes. Any attachments will automatically be saved within that file, but could also be saved separately if required. Non-Outlook users should store e-mails as .txt files, saving any attachments separately.
- 3) It is acceptable to print e-mails and store them in hard copy if required, although electronic storage is preferred for reasons of space, accessibility, disaster recovery, etc.
- 4) When e-mails are saved outside the e-mail system, it is recommended that they are renamed with the transmission date at the start of the title in the format DD-MM-YYYY, e.g. 16-05-2013 for an e-mail received on 16th May 2013. This simplifies their sorting by chronological order.



## E-Mail Access Policy

Document No. GIPCL/PL/18

Release Date: 23<sup>rd</sup> May 2020

- 5) It is usually only necessary to keep the latest e-mail in a chain of correspondence, as the preceding messages will be saved with it.
- 6) The use of personal e-mail archives (PST) is strongly discouraged. E-mails stored in such systems cannot easily be identified; they are not kept in their correct context, are not readily accessible by other staff, are usually retained indefinitely and may still be subject to external disclosure.
- 7) All e-mail folders, particularly the Junk Mail and Deleted Items folders should be purged regularly. For example, Deleted Items might be emptied at the beginning of each week and Junk Mail daily.

### 4.10 Maintaining Corporate Image

- 1) When using company resources to access and use the Internet, users must realize they represent the company. Whenever users state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".
- 2) Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the supervisor and will be placed by an authorized individual.
- 3) A standard, consistent and clean email signature will present a more professional appearance for our company. The email signature shall be designed by individual e-mail user to maximize contact information while also promoting external websites to those who receive our messages.

### 4.11 Security and Monitoring

- 1) Users should consider that their email activities are periodically monitored and limit their activities accordingly. Management reserves the right to examine e-mail at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.
- 2) Users who identify or perceive an actual or suspected security problem shall immediately contact the Operation Team as outlined in the Incident Reporting section of this policy.
- 3) Access to GIPCL network infrastructure and email resources shall be revoked for any user identified as a security risk or has a demonstrated history of security problems.

	<h2>E-Mail Access Policy</h2>	Document No. GIPCL/PL/18
		Release Date: 23 <sup>rd</sup> May 2020

### 4.12 Compliance

All terms and conditions as stated in this policy document are applicable to all users of the GIPCL network infrastructure. To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

All users must agree to abide by this Email Usage Policy. It is understood and taken for granted by the management of GIPCL that the users are made aware of the contents of this policy document as part of their induction process and agree to abide by its provisions.

### 4.13 Incident Reporting

Any complaints (other than claims of copyright or trademark infringement) regarding violation of this policy by a user should be directed to [cert@gipcl.com](mailto:cert@gipcl.com).

Where possible, include details that would assist the IT Team in investigating and resolving such complaint.

**On violations of this policy, management may take appropriate disciplinary action.**





# Malware Protection Policy

Document No. GIPCL/PL/19

Release Date: 23<sup>rd</sup> March 2020

# Malware Protection Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> March 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>



# Malware Protection Policy

Document No. GIPCL/PL/19

Release Date: 23<sup>rd</sup> March 2020

## Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23-March-2020	Prakash Binwal	D B Jani	Col S B Gurkha	Base line Initial Release



# Malware Protection Policy

Document No. GIPCL/PL/19

Release Date: 23<sup>rd</sup> March 2020

## Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Policy.....	4



# Malware Protection Policy

Document No. GIPCL/PL/19

Release Date: 23<sup>rd</sup> March 2020

## 1 Scope

All employees, interns, contractors, members, participants, users, and third parties who may have access or exposure to data are required to comply with this policy.

## 2 Purpose

To establish the requirements for the protection of information assets against intrusion by viruses and other malware.

## 3 Policy

### General guideline

#### Virus and Malware Protection Policy:

- Organisation shall protect its information assets by taking active measures to detect, prevent, and manage malware and virus intrusions and to recover from their effects.
- Organisation shall actively monitor traffic on the Organisation network and computing devices connected to the network, including remote activity and traffic, in order to maintain the integrity, reliability and performance of IT Systems. This includes (but is not limited to) monitoring for computer viruses and other malware, attempts to access the systems without appropriate authorization, systems performance, and compliance with policies.
- Organisation shall reserve the right to intercept and/or quarantine any network traffic or computing resources that may pose a threat to infrastructure, systems or data. This includes but is not limited to files, messages, network traffic and devices.

#### Controls Against Malicious Code:

- Detection, prevention, and recovery controls shall be implemented to protect against malicious code.
- Protection against malicious code shall be based on security awareness, appropriate system access controls, and change management controls.
- Anti-malware software shall be installed and operating on organisation all computing devices.
- Anti-malware software shall ensure that updates are applied within 24 hours of availability.



# Malware Protection Policy

Document No. GIPCL/PL/19

Release Date: 23<sup>rd</sup> March 2020

- Anti-malware software shall conduct scans of critical computing devices on boot and every 24hours.
- Organisation shall develop procedures that address the receipt of false positives during malicious code detection and eradication and the potential impact on the availability of the information system.
- Anti-malware software shall be configured to automatically scan the following:
  - Downloads from external sources
  - Files received over the network
  - Inbound email and attachments
  - Web traffic, such as HTML, JavaScript, and HTTP
- Anti-malware software shall create audit logs of all scans according to the Audit, Logging, and Monitoring Policy.
- Anti-malware software shall block or quarantine malicious code and send an alert to the System Administrator. Infected computing devices shall be removed from the Organisation network until they are verified as safe by the Chief Information Security Officer (CISO).
- Anti-spam software shall be implemented at the entry/exit points of the network and at computing devices connected to the Organisation network.
- Anti-spam software shall be updated when new releases are available in accordance with the Configuration Management Policy.
- Organisation shall periodically scan information systems to identify and, where possible, remove any unauthorized software.
- Procedures for responding to detections of malicious code and unauthorized software shall be developed.
- User functionality shall be separated from information system management functionality.
- Each entity shall attempt to identify computing devices that have been compromised and appropriately remediate.



## Malware Protection Policy

Document No. GIPCL/PL/19

Release Date: 23<sup>rd</sup> March 2020

- Once computing devices have been identified as compromised, security actions shall be initiated under the Incident Management Policy for affected computing devices. Virus and Malware Protection Policy.
- For systems not commonly affected by malicious software, each entity shall perform periodic assessments to confirm whether such systems continue to not require anti-virus software.
- External web sites, specific non-critical ports, and Internet Protocol (IP) addresses and ranges that are known sources of malware shall be blocked.

**On violations of this policy, management may take appropriate disciplinary action.**



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

# Log Management Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujarat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Prakash Binwal	D B Jani	Col S B Gurkha	Base line Initial Release





# Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

Overview .....	4
Protection of log information .....	5
Retention of Logs .....	5
Server Log Management .....	5
Firewall Log Management .....	6
Clock Synchronisation .....	7
IT Operations Monitoring .....	8



# Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

## Overview

### Event Logging

Event Logs shall be used to assist in troubleshooting, monitoring significant negative changes to system performance, record the actions of users when necessary to properly maintain security but without violating reasonable privacy expectations of legitimate users, give the ability to trend and track security instances, and provide data useful for investigating malicious activity.

A log management system shall be implemented that includes generating, transmitting, storing, analyzing, and disposing of computer log data, which shall:

- a. Create and maintain a secure log management infrastructure by balancing system performance, storage resources, and legal requirements;
- b. Commit resources to perform timely log review;
- c. Identify roles and responsibilities of staff associated with this process;
- d. Develop standards, procedures, and guidelines as needed to support this program;
- e. Retain the logs based on business requirements.

Event logs shall include, when relevant:

- a. user IDs;
- b. system activities;
- c. dates, times and details of key events, e.g. log-on and log-off;
- d. device identity or location;
- e. records of successful and rejected system access attempts;
- f. records of successful and rejected data and other resource access attempts;
- g. changes to system configuration;
- h. use of privileges;



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

- i. use of system utilities and applications;
- j. files accessed and the kind of access;
- k. network addresses and protocols;
- l. alarms raised by the access control system;
- m. activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems (IDS);
- n. records of transactions executed by users in applications.

### Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access. System logs need to be protected, because if the data can be modified or data is deleted, their existence may create a false sense of security.

Unauthorized changes to log information and operational problems with the logging facility shall be protected.

### Retention of Logs

- ❖ Firewall logs -1 week on device-manual deletion,  
90 days backup-manual deletion of previous logs
- ❖ Database logs - As per Backup & Restoration Plan

### Systems & Administrator logs

Systems & Administrator activities shall be logged and regularly reviewed.

### Server Log Management

All production servers with windows operating system are configured for managing logs as follows:

- Over-writing of event logs is enabled;
- Logs of Application, Security and System events are captured and monitored;
- All reported errors are documented and resolved;



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

➤ Backup of logs are generally not taken.

Following known errors where resolution is not required, but limited to:

- ✘ Driver Microsoft XPS Document Writer required for printer Microsoft XPS Document Writer is unknown. Contact the administrator to install the driver before you log in again.
- ✘ MRxSmb - The redirector failed to determine the connection type.
- ✘ Windows saved user registry while an application or service was still using the registry during log off. The memory used by the user's registry has not been freed. The registry will be unloaded when it is no longer in use.
- ✘ Client printer auto-creation failed. The driver could not be installed. Possible reasons for the failure: The driver is not in the list of drivers on the server.

### Firewall Log Management

Logs of all the firewalls are shipped and stored in Backup Server for future reference.

Firewall logs are copied and stored in separate System.

Firewall events are categorized as follows: -

SN	Category	Related events	Resolution	Process Action
1.	Emergency	Hardware Failure	Immediate resolution	To be brought in incident management
2.	Alert	Intrusion Detected	Analyze the alert and action will be taken in proactive manner	Preventive action management
3.	Critical	Configuration Changes	Immediate resolution	To be brought in incident management
4.	Error	L2TP/PPTP/PPPoE errors	Error will be observed & analyzed and proactive action will be taken	Correction and corrective action will be initiated



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

SN	Category	Related events	Resolution	Process Action
5.	Warning	Violation of Traffic	Warning will be observed and action will be taken, if required	Correction and corrective action will be initiated before any resolution.
6.	Notification	Configuration Changes	Notification will be observed and analyzed, if required	
7.	Information	authentication failure	No action required	

### Clock Synchronisation

The clocks of all relevant information processing systems shall be synchronized with single reference time source.

The correct setting of computer clocks shall be ensured for accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

A network time protocol shall be used to keep the servers & network devices in synchronization with the master clock.

The Master Clock & Standard Reference Time for use shall be -

Master Clock	OS Type	Standard Reference Time	Devices
	Linux	NTP Server	Network devices (Routers, Switches, IP Phones)
<b>x</b>	Windows	AD Server	All window based Servers, PCs & Laptops



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

### IT Operations Monitoring

Monitoring and logging devices and software shall be protected from unauthorized use and other internal or external attacks that may deactivate the logging process and/or modify to delete the logs themselves.

Logging facility and logs of monitored devices shall be protected from tampering and unauthorized access. The logs shall be securely stored to provide evidences during audits.

In the event of a faults and security incident, these logs shall be used for investigation, prosecution and disciplinary action.

Periodical audit and review of all logs generated shall be monitored.

Current list of user access privileges for Servers & Network devices shall be retained.

Company reserves the right to report any illegal activities to appropriate authorities and take legal action in case of legal breach. The legal department shall assist GIPCL in such instances.

Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- a. Internet traffic
- b. Electronic mail traffic
- c. LAN traffic, protocols, and device inventory
- d. Operating system security parameters

The following files shall be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- a. Automated intrusion detection system logs
- b. Firewall logs
- c. User account logs
- d. Network scanning logs
- e. System error logs



## Log Management Policy

Document No. GIPCL/PL/20

Release Date: 23<sup>rd</sup> May 2020

- f. Application logs
- g. Data backup and recovery logs
- h. Help desk trouble tickets

The following system checks/audit shall be performed at least annually:

- a. Password strength
- b. Unauthorized network devices
- c. Unauthorized personal web servers
- d. Unsecured sharing of devices
- e. Operating System and Software Licenses

Any security issues discovered shall be reported to CISO for follow-up investigation.

Events capturing should be done following ways

- a. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - ✓ Security related logs shall be kept online (in system) for a minimum of 1 month.
  - ✓ Security related logs shall be kept offline (in tapes) for a minimum of 6 months.
- b. Security-related events shall be monitored & corrective measures shall be taken as needed. Security-related events include, but are not limited to:
  - ✓ Port-scan attacks;
  - ✓ Evidence of unauthorized access to privileged accounts;
  - ✓ Anomalous occurrences that are not related to specific applications on host.

**On violations of this policy, management may take appropriate disciplinary action.**



## Encryption Policy

Document No. GIPCL/PL/21

Release Date: 23<sup>rd</sup> March 2020

# Encryption Policy



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> March 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujrat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>



	<h1>Encryption Policy</h1>	Document No. GIPCL/PL/21
		Release Date: 23 <sup>rd</sup> March 2020

## Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23-March-2020	Prakash Binwal	D B Jani	Col S B Gurkha	Base line Initial Release

## Table of Contents

1	Purpose .....	4
2	Scope .....	<b>Error! Bookmark not defined.</b>
3	Policy.....	<b>Error! Bookmark not defined.</b>
3.1	Asset Identification & Classification .....	<b>Error! Bookmark not defined.</b>
3.2	Classification of Information Assets .....	<b>Error! Bookmark not defined.</b>
3.3	Labelling of Physical Assets.....	<b>Error! Bookmark not defined.</b>
3.4	Labelling of Documents .....	<b>Error! Bookmark not defined.</b>
3.5	Handling of Information Assets .....	<b>Error! Bookmark not defined.</b>



# Encryption Policy

Document No. GIPCL/PL/21

Release Date: 23<sup>rd</sup> March 2020

## Purpose

The policy on cryptographic controls includes procedures to provide appropriate levels of protection to Confidential or Restricted information whilst ensuring compliance with statutory, regulatory and contractual requirements.

Cryptographic controls shall be used to achieve different security objectives, e.g.:

- a. **Confidentiality:** using encryption of information to protect sensitive or critical information, either stored or transmitted;
- b. **Integrity/Authenticity:** using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
- c. **Non-repudiation:** using cryptographic techniques to obtain proof of the occurrence or nonoccurrence of an event or action.
- d. **Authentication:** using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.
  1. Confidential or Restricted information shall only be imported to or taken for use away from the organization in an encrypted form.
  2. Authorized staff shall be able to gain access, when needed, to any relevant information held in encrypted form.
  3. The confidentiality of information being imported or transferred on portable media or across networks must be protected by use of appropriate encryption techniques.
  4. Encryption shall be used whenever appropriate on all remote access connections to the GIPCL's network and resources.
  5. Key management shall be in place to support the organization's use of cryptographic techniques.

	<h2>Encryption Policy</h2>	Document No. GIPCL/PL/21
		Release Date: 23 <sup>rd</sup> March 2020

- a. Recommended key size is 128 bits and 256 bits.
- b. Following encryption algorithms shall be used:
  - Triple DES
  - RC4
  - AES
  - MD5
  - RSA (protocol used are TNS and SSL-VPN)
  - SHA-1
  - Group 1, 2, 5, 7 (used in firewall)
6. Authenticity of public keys shall be done using public key certificates.
7. Use of digital signatures shall be restricted for e-bidding. Persons handling the e-bidding module shall be personally responsible for the secure use and protection of their private key.

**On violations of this policy, Management may take appropriate disciplinary action.**

	<h2>Change Management Policy</h2>	Document No. GIPCL/PL/22
		Release Date: 23 <sup>rd</sup> March 2020

<h2>Change Management Policy</h2>	
	
<p>This document is the property of Gujarat Industries Power Co. Ltd.</p>	
Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> March 2020
<p>Gujarat Industries Power Co. Ltd. P.O. Petrochemical, Vadodara, Gujarat -391346 Tele: +91 265 2232768 Fax: +91 265 2230029 Website: <a href="http://www.gipcl.com">http://www.gipcl.com</a></p>	

	<h2>Change Management Policy</h2>	Document No. GIPCL/PL/22
		Release Date: 23 <sup>rd</sup> March 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23-March-2020	Prakash Binwal	D B Jani	Col S B Gurkha	Base line Initial Release



# Change Management Policy

Document No. GIPCL/PL/22

Release Date: 23<sup>rd</sup> March 2020

## Table of Contents

1	Introduction .....	4
2	Scope of Change Management .....	5
2.1	Definition.....	5
2.2	Examples of Changes in Scope .....	6
2.3	Examples of Changes Out of Scope .....	6
2.4	Changes to Software Packages.....	7
3	Categories of Change .....	8
3.1	Standard change.....	8
3.2	Normal Changes.....	8
3.3	Emergency Changes.....	8
3.4	Major Changes .....	8
4	Raising, Assessment and Approval of Changes.....	9
4.1	Information to be supplied on Change Requests.....	9
4.2	Assessment of Changes.....	9
4.3	Approval of Changes.....	10
5	Reporting and Review .....	10



## 1 Introduction

The objective of the change management process is to ensure that changes to GIPCL IT services and their associated components are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Reliability and business continuity are essential for the success and survival of any organization and are particularly important in our environment.

Change Management enables GIPCL Operations to add value to the business by:

- Prioritizing and responding to business and customer change proposals
- Implementing changes that meet the customers' agreed service requirements while optimizing costs.
- Contributing to meet governance, legal, contractual and regulatory requirements
- Reducing failed changes and therefore service disruption, defects and re-work
- Delivering change based on urgency and business benefit
- Contributing to better estimations of the quality, time and cost of change
- Assessing the risks associated with the transition of services
- Aiding productivity of staff through minimizing disruptions due to high levels of unplanned or 'emergency' change, hence maximising service availability
- Reducing the Mean Time to Restore Service (MTRS), via quicker and more successful implementations of corrective changes





## 2 Scope of Change Management

### 2.1 Definition

All hardware, software and documentation that constitute a live service to GIPCL users will be subject to change management. The exception is where certain types of change have been designated as standard changes and implemented via the service request process.

As an indication, changes to the following will require a change request to be raised and approved:

- Server hardware
  - New installations onto the live network
  - Upgrades
  - Decommissioning
- Server operating software including
  - Upgrades
  - Fixes and service packs
  - Configuration changes
- Application softwares
  - Upgrades
  - Fixes
  - Configuration changes
- Firewalls
- Routers
- Switches
- Network services e.g. DNS, DHCP

	<h2>Change Management Policy</h2>	Document No. GIPCL/PL/22
		Release Date: 23 <sup>rd</sup> March 2020

### 2.2 Examples of Changes in Scope

The following are examples of recently implemented or planned changes that will in future require a change request to be raised and approved:

1. Applying outstanding fixes to the Exchange system
2. Installing the Exchange servers onto the live network
3. Installing the VPN router onto the live network
4. Installing SCCM onto a server connected to the live network
5. installing a new network component in the live environment

### 2.3 Examples of Changes Out of Scope

The following but not limited to are some of examples tasks that are considered to be service requests or administrative tasks and so will not require a change request to be raised and approved:

1. Creating a new user
2. Changing a user's password (password reset)
3. Mapping a drive for a user
4. Installing individual new PCs
5. Upgrading memory in an individual PC
6. Installing software on a user's desktop

	<h2>Change Management Policy</h2>	Document No. GIPCL/PL/22
		Release Date: 23 <sup>rd</sup> March 2020

### 2.4 Changes to Software Packages

It is GIPCLs policy to use, where possible, commercial off-the-shelf (COTS) software packages to fulfil business requirements for information systems.

Where such packages are used they should, as far as possible, not be subject to modification by GIPCL. Such modification carries the following risks:

- The integrity of the software application may be affected by changes
- Future updates from the software vendor may become more difficult to apply
- Integration with other software packages may be affected

If changes are felt to be absolutely necessary because of some bug or a new functionality / feature in the product, it is the policy of GIPCL to request that they be made and supported by the vendor of the software package as standard features of their product. For the changes to be applied, the approval is provided by DGM IT.

After the review & detailed understanding of the requirement from the user DGM IT approves the changes & then it is passed on to vendor for development. Again the same approach is followed of testing in the test server & then getting it deployed on the production server.

	<h1>Change Management Policy</h1>	Document No. GIPCL/PL/22
		Release Date: 23 <sup>rd</sup> March 2020

### 3 Categories of Change

In order to decide which, route a change should take through the process, change requests will be categorised based on its estimated resource requirement, urgency and risk.

The following categories of change will be used:

#### 3.1 Standard change

A standard change is a small, low risk change that can be implemented in a short governed timeframe. Although a standard change is technically a change, it will not require a change request to be assessed and approved, although it should still be logged against the relevant configuration item as having taken place. Some standard changes will be requested by users via the service request process.

#### 3.2 Normal Changes

A normal change is one which has not been pre-classified as a standard change, is not an emergency and does not meet the criteria for a major change. Normal changes will be subject to the change management process.

#### 3.3 Emergency Changes

Emergency changes are changes which are urgently required in order to resolve a major incident or problem. These will be fast-tracked through the change management process and given additional resource where required. Note that a failure in forward planning to log a normal change in enough time to obtain approval does not constitute an emergency change and will not be treated as such.

#### 3.4 Major Changes

Changes that have the potential to have a major impact on a service, although still logged as change requests and tracked via the change management process, will be handled via the Design and Transition of New or Changed Services process.

	<h2 style="margin: 0;">Change Management Policy</h2>	Document No. GIPCL/PL/22
		Release Date: 23 <sup>rd</sup> March 2020

These will be planned and managed as projects and the following criteria will be used to assess whether a proposed change is classified as major.

A change will be classified as major if it involves any or all of:

1. the removal or decommissioning of a service
2. the transfer of a service from a vendor to the business or a different party
3. the creation of a new service

These criteria will be re-evaluated on a regular basis as part of a wider change management process review.

## 4 Raising, Assessment and Approval of Changes

### 4.1 Information to be supplied on Change Requests

The following items of information must be supplied on a change request in order for it to be processed and approved. Change requests not containing this information will be rejected.

- Initiator name and contact details
- Summary of change
- Change Description
- Business Justification
- Service(s) Affected
- Impact
- Urgency

Relevant documentation should be attached to the change record if required.

### 4.2 Assessment of Changes

Changes must be assessed from the dual perspective of technical and business risk. For many changes this will mean that at least two members of staff will need to be



## Change Management Policy

Document No. GIPCL/PL/22

Release Date: 23<sup>rd</sup> March 2020

involved - one technical, the other business. This should include the timing of the proposed change and its potential impact on security, capacity, service continuity plans and release management, amongst other areas. Change Initiators must not assess their own changes. The technical assessor must have sufficient technical knowledge to be able to give an informed opinion regarding the change subject.

### 4.3 Approval of Changes

The approval of changes is done by DGM (IT) for the technical & functional aspects & CFO for Financial aspects.

Change Initiators must not approve their own changes. Where possible the assessors of a change should be different to the approver(s).

## 5 Reporting and Review

The success of changes will be reviewed at an appropriate time after their implementation to judge their success or otherwise.

The success of the change should be reviewed with regard to whether:

- the change met the required objectives, standards and functionality
- users and customers are happy with the results
- the change was implemented as per the planned resources, agreed schedules and anticipated costs
- there are related incidents or problems since the change was implemented
- there were unexpected side effects
- There are opportunities to improve the next similar change

The changes applied to the production system by IT team & formally the issue ticket is closed in support tool.

# **Index**

1. Management review process
2. Monitoring Measure and Evaluation Process
3. Control of Records Process
4. Visitor Access Process
5. Legal Compliance Process
6. Continual Improvement Process
7. Data Security Process
8. Vulnerability Management Process



## Management Review Process

Document No. GIPCL/ISMS/PR/01

Release Date: 23<sup>rd</sup> May 2020

# Management Review Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujarat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**



	<h2>Management Review Process</h2>	Document No. GIPCL/ISMS/PR/01
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



## Management Review Process

Document No. GIPCL/ISMS/PR/01

Release Date: 23<sup>rd</sup> May 2020

### Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Procedure .....	4
4	Roles and Responsibility.....	4
5	Procedure Invocation .....	5



# Management Review Process

Document No. GIPCL/ISMS/PR/01

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This procedure applies to all staff/ users that are directly or indirectly employed by Organization, subsidiaries or any entity conducting work on behalf of Organization that involves the use of information assets.

## 2 Purpose

The Purpose of Management Review Procedure is to ensure its continuous suitability, adequacy and effectiveness. The review includes assessing opportunities for improvement and the need for change. The results of the reviews shall be clearly documented and records maintained.

## 3 Procedure

### General guideline

Compliance with this procedure is mandatory ensure continuous compliance monitoring within their departments. Compliance with the statements of this procedure is a matter of periodic review by Risk & Information Security Department and any violation of the procedure will result in corrective action by the ISMS Committee.

## 4 Roles and Responsibility

Each role involved in this procedure shall have main responsibilities as follows:

### 1. ISMS Manager

- Reviewing Information security Policies and procedures, evaluate and follow up Implementation.
- Reviewing Information security Policies and procedures on annual basis for update/modification/effectiveness.

### 2. Information Security Officer

- Develop information security procedures in compliance with information security policy.
- Updating and maintaining information security policies and procedures periodically
- Deploying modifications to information security procedures.
- Maintaining an accurate update/ modification/ deletion record of information security policies and procedures.

### 3. Human Resource Department

- Inspects all documents for regulatory / legal issues in compliance with policy.



## Management Review Process

Document No. GIPCL/ISMS/PR/01

Release Date: 23<sup>rd</sup> May 2020

### 5 Procedure Invocation

This procedure shall be followed whenever there is:

- Follow up actions from previous management meeting.
- Results of security audits and reviews.
- Actions which could improve information security management.
- Vulnerabilities or threats not adequately addressed in previous risk assessment.
- New vulnerabilities or threats identified.
- Incidents handling.
- Feedback from interested parties.
- Changes that could affect information security management.
- Recommendations for improvement.

**On violations of this policy, management may take appropriate disciplinary action.**



## Monitor measure and Evaluation Process

Document No. GIPCL/ISMS/PR/02

Release Date: 23<sup>rd</sup> May 2020

# Monitor measure and Evaluation Process





## Monitor measure and Evaluation Process

Document No. GIPCL/ISMS/PR/02

Release Date: 23<sup>rd</sup> May 2020

This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<b>Monitor measure and Evaluation Process</b>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

## Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release

	<b>Monitor measure and Evaluation Process</b>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

## Table of Contents

1	Scope .....	5
2	Purpose.....	5
3	Procedure .....	5
4	Roles and Responsibility.....	5
5	Importance of Staff Participation .....	6
6	Evaluation Plan .....	7
6.1	Mandates for evaluation.....	7
6.2	Definition and purpose of evaluation.....	7
7	Roles and responsibility .....	9



	<h2>Monitor measure and Evaluation Process</h2>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

### 1 Scope

This procedure applies to all staff/ users that are directly or indirectly employed by Organization, subsidiaries or any entity conducting work on behalf of Organization that involves the use of information assets. Monitoring is defined as” a continuing function that uses systematic collection of data on specified indicators to provide management and the main stakeholders of an ongoing development intervention with indications of the extent of progress and achievement of objectives and progress.

### 2 Purpose

The Purpose of Monitor measure and Evaluation Process is to Monitoring and evaluation are integral components of function as distinct mechanisms for oversight and accountability. Performance monitoring measures progress towards achieving results planned for in programmes and projects; while evaluation assesses the worth of an intervention.

### 3 Procedure

#### Use of monitoring

The interim and end-of-cycle reporting focuses on outcomes or objective. Monitoring is therefore a key element in the results-based management chain.

Results from monitoring are used by Organization

- Improve sub programme and project management, by identifying and taking corrective action(s), as required, to ensure that objectives are met within a given budget and timeframe by comparing actual progress against initial plans;
- Support organizational learning, inform decision-making and strengthen future strategic and programme planning by documenting and sharing findings and lessons learned internally and externally.

### 4 Roles and Responsibility

Monitoring responsibilities are described in the job descriptions of relevant staff members and specific monitoring tasks should be included in their performance appraisal.

#### The Executive Secretary and Deputy-Executive Secretaries

These are responsible for overseeing the work of the divisions, sub regional offices and regional institutions, and are accountable to member States for the achievements.

	<h2>Monitor measure and Evaluation Process</h2>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

Senior managers are also required to meet with the Executive Secretary to report on the annual work plan of their respective division (and related regional institution) and sub regional office, as well as on the accomplishment accounts of their respective sub programme.

### **Heads of division and sub-regional office**

These are responsible for managing the programme of work of their respective subprogramme including monitoring functions. In particular, they approve divisional submissions related to monitoring before sending them to the Strategy and Programme Management Division (SPMD).

### **Officers**

Responsible for the implementation of projects or activities under the subprogramme should routinely monitor their progress.

### **Planning, monitoring and evaluation (PME) focal points**

In each division and sub regional office advise all colleagues, including senior managers, on monitoring-related matters in order to strengthen the internal capacity to address these issues; coordinate and review submissions related to monitoring before sending them to SPMD; and act as focal point for communication on monitoring with SPMD.

### **The Strategy and Programme Management Division (SPMD)**

Plays a technical support and coordinating role and, together with the Department of Management, has a quality assurance function.

**The Department of Management**, and in particular the Policy and Oversight Coordination Service, Office of the Under-Secretary General, provides support and quality assurance in monitoring the programme of work.

## **5 Importance of Staff Participation**

Active staff involvement in planning and monitoring will enhance ownership of the process and thus facilitate the achievement of results. Staff participation also encourages the sharing of experiences, which strengthens organizational learning. Heads of division and sub regional office should ensure active staff involvement at all stages of the programme cycle, but particularly during the preparation of the following:

	<h2>Monitor measure and Evaluation Process</h2>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

**Annual work plan:** As staff members are responsible for the day-to-day delivery of outputs, they are best placed to determine how much time is needed for each activity, and to set realistic deadlines. As such, the annual work plan preparation can be used as a basis for the e-performance document plan for individual staff members.

**Accomplishment accounts:** Staff members can provide an update on the delivery of outputs, achievements against pre-set indicators, constraints encountered and how these are managed, and lessons learned and suggestions for follow-up and improvement. This feedback should strengthen the overall delivery of the programme of work while contributing to the development of capacity for all staff members. It can also be used to update the annual work plan and for the review of staff performance in e-performance document.

**Programme performance report (PPR):** Staff members can provide similar inputs as during the preparation of accomplishment accounts. However, the PPR is even more important in that it effectively reflects on the entire programme cycle and is used to inform the planning process for future strategic frameworks. In addition, the programme performance report is shared with member States. The PPR is thus also a time for reflecting jointly on lessons learned, including from evaluations conducted during the biennium.

**Project monitoring:** Staff members are responsible for monitoring the progress of projects on a day-to-day basis. This could include, for example, tracking the preparation of workshops, funds committed and spent, and the delivery of outputs by consultants and project partners. In addition, they ensure that progress of projects is monitored based on the project document and monitoring and reporting milestones are undertaken effectively and in a timely manner.

## 6 Evaluation Plan

### 6.1 Mandates for evaluation

The work of divisions, sub regional offices and regional institutions. On certain occasions, member States also mandate the secretariat through a resolution to conduct an evaluation of a specific theme or area of work in support of its decision-making processes.

### 6.2 Definition and purpose of evaluation

The purposes of evaluation are to promote accountability and learning, and support results-based management. Evaluation aims to understand why and to what extent intended and unintended

	<b>Monitor measure and Evaluation Process</b>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

results were achieved; and to analyse the implications of the results. Evaluation can inform planning, programming, budgeting, implementation and reporting and can contribute to evidence-based policymaking, development effectiveness and organizational effectiveness.

	<h2>Monitor measure and Evaluation Process</h2>	Document No. GIPCL/ISMS/PR/02
		Release Date: 23 <sup>rd</sup> May 2020

## 7 Roles and responsibility

The following organizational roles and responsibilities are as follows:

- **The Commission:** Responsible for guidance and oversight of work. The Commission may request evaluations through resolutions. Committees subsidiary to the Commission may recommend an evaluation to the Commission.
- **The Executive Secretary:** Assumes a critical leadership role in ensuring an empowered evaluation function, with sufficient resources to carry out periodic evaluations and use evaluation findings to enrich strategic planning, improve organizational learning and strengthen accountability.
- **Senior management:** Accountable for the implementation of follow-up to evaluations outlined in management responses and follow-up action plans.
- **Evaluation Unit, Strategy and Programme Management Division (SPMD):** Organization established a dedicated Evaluation Unit in the SPMD to ensure an effective management of evaluation function, the conduct of independent, credible and useful evaluations and the use of evaluation findings and recommendations for accountability and organizational improvement.

**On violations of this policy, management may take appropriate disciplinary action.**

	<b>Control of Records Process</b>	Document No. GIPCL/ISMS/PR/03
		Release Date: 23 <sup>rd</sup> May 2020

# Control of Records Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujarat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Control of Records Process</h2>	Document No. GIPCL/ISMS/PR/03
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jani	Col S B Gurkha	Base line Initial Release



# Control of Records Process

Document No. GIPCL/ISMS/PR/03

Release Date: 23<sup>rd</sup> May 2020

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Process.....	4
4.1	Records Lifecycle.....	4
4.1.1	Identification .....	4
4.1.2	Storage .....	5
4.1.3	Protection .....	5
4.1.4	Retrieval.....	5
4.1.5	Retention.....	5
4.1.6	Disposal .....	6





# Control of Records Process

Document No. GIPCL/ISMS/PR/03

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

The ISO/IEC 27001 standard requires that all records that make up the Information Security Management System (ISMS) must be controlled. Such control is essential in order to ensure that the correct processes and procedures are in use at all times within the organisation and that they remain appropriate for the purpose for which they were created.

The general principles are that all documented information must be:

- Readily identifiable and available
- Dated, and authorised by a designated person
- Legible and readable
- Maintained under version control and available to all locations where service management activities are performed
- Promptly withdrawn when obsolete and retained in/as an archive where required for legal or knowledge preservation purposes, or both

This procedure sets out how this level of control will be achieved within GIPCL.

## 2 Purpose

This document describes the controls in place for the creation, management and disposal of records within the ISMS.

## 3 Scope

This process applies to all the records (documented information) created during the business processes.

## 4 Process

### 4.1 Records Lifecycle

#### 4.1.1 Identification

There is a variety of types of record that make up the ISMS and these will be associated with the specific processes that are involved, such as:

- Security Incidents
- Changes
- Configuration items



## Control of Records Process

Document No. GIPCL/ISMS/PR/03

Release Date: 23<sup>rd</sup> May 2020

- Security Event logs

In addition there will be more general items such as meeting minutes which could apply across processes.

For those records that are manually created the following rules will apply:

- Meeting minutes will be named according to the subject of the meeting and the date
- Reports will be named according to the subject of the report and the reporting period
- Logs will be named with the title of the log and the date/time period covered

For any other types of record not covered, the creator should use common sense to ensure that the name chosen gives a good indication as to the contents of the file and it should be stored in a location relevant to its purpose.

### 4.1.2 Storage

Many records within the ISMS will be stored in application databases specifically created for the purpose e.g. the security incident database.

For non-database records, a logical filing structure will be created according to the area of the ISMS involved.

[Describe the filing structure on your server in which you will store your ISMS records]

Where possible, all records will be held electronically; paper documents should be scanned in if an original electronic copy is not available.

### 4.1.3 Protection

Records held in application databases will be subject to regular backups as part of the organisation's IT service continuity procedures. File storage areas will also be backed up regularly, with all latest backups held at an offsite location.

Access to the records will be restricted to authorised individuals in accordance with the GIPCL Information Security Policy.

### 4.1.4 Retrieval

Records will generally be retrieved via the application that created them e.g. the service desk system for incidents, problems etc. and a word processor for documents.

Reporting tools will also be used to process and consolidate data into meaningful information

### 4.1.5 Retention

The period of retention of records within the ISMS will depend upon their usefulness to the [Service Provider] and its customers. Security-related service desk records are useful for historical trend

	<b>Control of Records Process</b>	Document No. GIPCL/ISMS/PR/03
		Release Date: 23 <sup>rd</sup> May 2020

analysis and so will be kept for a period of at least 7 years. Particular care will be taken where records may have some commercial relevance in the event of a dispute e.g. contracts and minutes of meetings with suppliers and these should be kept for the same length of time.

Records that are particularly detailed and only relevant for a short period of time such as server event logs should only be kept as long as there is an immediate requirement for them.

#### **4.1.6 Disposal**

Many systems provide for the concept of archiving and in most cases this should be used rather than deletion. However once it has been decided to dispose of a set of records they should be deleted using the appropriate software e.g. the service desk system will provide a facility to delete incident records.

If such records are held on hardware that is also to be disposed of then all hard disks must be shredded by an approved contractor.

Paper copies of records that are to be disposed of should be shredded in line with the organisation's information security policy.



## Visitor Access Process

Document No. GIPCL/ISMS/PR/04

Release Date: 23<sup>rd</sup> May 2020

# Visitor Access Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

**Gujarat Industries Power Co. Ltd.**  
**P.O. Petrochemical, Vadodara, Gujarat -391346**  
**Tele: +91 265 2232768**  
**Fax: +91 265 2230029**  
**Website: <http://www.gipcl.com>**

	<h2>Visitor Access Process</h2>	Document No. GIPCL/ISMS/PR/04
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release

## Table of Contents

1	Overview .....	4
2	Purpose .....	4
3	Scope.....	4
4	Process.....	4
4.1	Common Procedure .....	4
4.2	Procedure Exclusive for AKS IT NOIDA- ISACC Services Work Area .....	6



# Visitor Access Process

Document No. GIPCL/ISMS/PR/04

Release Date: 23<sup>rd</sup> May 2020

## 1 Overview

Organisation hosts various critical assets in its premises. These critical assets are in turn are managed, maintained by the responsible personnel. There are a lot of occasion when there is need for a 3<sup>rd</sup> party individual, vendors, housekeepers, utility members will require access to the areas hosting these assets. Therefore it is required to clearly identify and distinguish these outside individuals from the ones those are employees of the organisation.

## 2 Purpose

This procedure defines the Visitor Access Procedure with the requirements of Clause 11 (Physical and Environmental Security) of ISO 27001:2013.

## 3 Scope

This policy applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to GIPCL systems.

## 4 Process

The procedure for visitor access to AKS IT NOIDA - ISACC Services will be explained in two parts, one common procedure for access of all visitors to AKS IT NOIDA and the second, and the exclusive procedure for access to the AKS IT NOIDA - ISACC Service Work Premises.

### 4.1 Common Procedure

- All visitors will report at the AKS IT NOIDA's Reception Desk.
- At the Reception, the visitor will be requested to make entries in the Visitor Log Book.
- The Visitors Log Book will have the following columns:
  - Sr.No.
  - Date
  - Name of the visitor
  - Officer to meet, with designation Reason; Official or Personal
  - Time-in and Time-out
  - Signature of the visitor
  - Signature of the officer escorting the visitor



## Visitor Access Process

Document No. GIPCL/ISMS/PR/04

Release Date: 23<sup>rd</sup> May 2020

- On completion of entries the receptionist will speak to the employee to be visited and take instructions whether he/she will come down personally to escort the visitor, send someone or come down to meet the visitor in the Reception Area or in Conference Room.
- Invariably, no visitor should be permitted to enter the work area, unless with the explicit permission of the Admin Officer.



	<h2>Visitor Access Process</h2>	Document No. GIPCL/ISMS/PR/04
		Release Date: 23 <sup>rd</sup> May 2020

#### 4.2 Procedure Exclusive for AKS IT NOIDA- ISACC Services Work Area

- The procedure elucidated above, will be followed for visitors requesting access to the AKS IT NOIDA- ISACC Services Premises.
- The visitor will be mandatorily escorted by a Security Personal /Employee of the AKS IT NOIDA.
- For visitors being allowed access to the AKS IT NOIDA- ISACC Services Work Area, the following entries must be made in the Visitors Log Book, prior to the visitor entering the AKS IT NOIDA- ISACC Services Work Area:
  - Sr.No.
  - Name of the visitor
  - Organization being represented by the visitor
  - Officer to meet, with designation
  - Pen drive/Storage Media/Laptops(S/N)
  - Time-in and Time-out
  - Signature of the visitor
  - Signature of the officer escorting the visitor
  - Identity Card Number
- The visitor will be escorted out of the AKS IT NOIDA- ISACC Services Work Area, till the Reception, and the Time-out endorsed on the Visitor Log Book.



## Legal Compliance Process

Document No. GIPCL/ISMS/PR/05

Release Date: 23<sup>rd</sup> May 2020

# Legal Compliance Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Legal Compliance Process</h2>	Document No. GIPCL/ISMS/PR/05
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



## Legal Compliance Process

Document No. GIPCL/ISMS/PR/05

Release Date: 23<sup>rd</sup> May 2020

### Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Procedures.....	4
4	Identify Requirement .....	6
5	Access.....	6
6	Assess Implications.....	6
7	Document Requirement .....	7
8	Communicate to Interested Parties .....	7
9	Review.....	7
10	Update.....	7



# Legal Compliance Process

Document No. GIPCL/ISMS/PR/05

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This policy covers the applicable legal and regulatory requirements relevant to ISMS will be access, documented and communicated by Organizations.

## 2 Purpose

This document sets out how the applicable legal and regulatory requirements relevant to the ISMS will be identified, accessed, assessed, documented, maintained and communicated.

[Organisation Name] has implemented an Information Security Management System (ISMS) in line with the ISO/IEC 27001 international standard for information security management.

In creating and maintaining an ISMS it is vital that a full understanding is gained of the various legal and regulatory requirements that apply to [Organisation Name] and its business. This will ensure that the organisation continues to meet its obligations and its board of directors and other stakeholders are not exposed to the risk of criminal prosecution or corporate liability.

The purpose of this procedure is to document how such requirements are identified and incorporated into the ISMS and how updates to the requirements are handled.

## 3 Procedures

### General guideline

The specifics of the procedure will depend upon the legal and regulatory environment in which your organisation operates.

You may well need to obtain legal advice, either from your internal legal team or an external law firm about which laws affect your business operations. If you operate in more than one country then local advice will need to be sought from each country individually.

This procedure defines the steps need at a fairly high level. You will need to add more organisation-specific detail to ensure it represents a useful procedure that reflects the way you have decide to approach this area.



# Legal Compliance Process

Document No. GIPCL/ISMS/PR/05

Release Date: 23<sup>rd</sup> May 2020

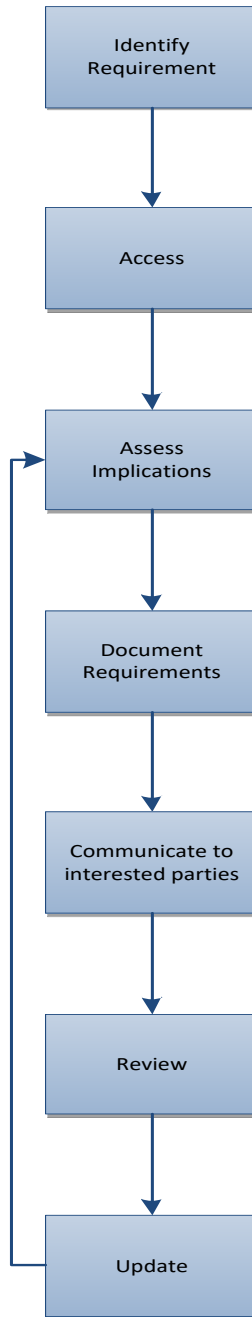


Figure 1 - Legal and regulatory requirements procedure



## Legal Compliance Process

Document No. GIPCL/ISMS/PR/05

Release Date: 23<sup>rd</sup> May 2020

### 4 Identify Requirement

[Organisation Name] relies upon the following internal teams and external bodies to identify legal and regulatory requirements that are relevant to its business operations:

Team/organisation	Areas Covered	Method of Communication
Legal department	Health and Safety Product Safety	Email alerts Six-monthly meetings
Information Security team	Data Protection	Email alerts Six-monthly meetings
Industry body	Various	Seminars Annual Conference
Regulatory Authority	Regulatory reporting	Official communications Briefing events

[Include all real or potential sources of advice in the above table]

### 5 Access

In general [Organisation Name] will rely upon the appropriate team or external body to provide an interpretation of the relevant parts of the item under consideration. This may be in the form of briefing papers or presentation materials.

Where necessary, the [IS Manager] shall obtain full copies of the relevant source material (such as Acts of Law or Regulatory announcements) for reference purposes. These may be in hardcopy or electronic form.

### 6 Assess Implications

The [IS Manager] is responsible for ensuring that a full assessment of the implications of the relevant items is carried out. This will be based upon qualified advice from the relevant source above. The assessment will include the following aspects:

- Degree of change to the ISMS and its associated policies. strategies and plans needed to meet the requirement
- Urgency of meeting the requirement
- Consequences of not meeting the requirement

	<b>Legal Compliance Process</b>	Document No. GIPCL/ISMS/PR/05
		Release Date: 23 <sup>rd</sup> May 2020

- Options for meeting the requirement

## 7 Document Requirement

Once assessed, the relevant requirements will be documented as part of the ISMS within the document ISMS04001 Information Security Context, Requirements and Scope. All changes to this document will be recorded in accordance with the ISMS documentation procedures.

Where possible, confirmation of the interpretation of the requirement will be obtained from a relevant source e.g. the organisation legal department.

## 8 Communicate to Interested Parties

Where immediate changes are needed to the ISMS as a result of a new or changed requirement these will be incorporated as soon as possible and revisions issued to all recipients of the relevant policies and procedures. Otherwise the change will be considered at the next annual review of the ISMS.

## 9 Review

All relevant requirements will be re-assessed on at least an annual basis as part of the ISMS annual review. Appropriate advice will be obtained at this point to ensure that all changes have been captured.

## 10 Update

Any new or changed requirements identified as part of the review will be handled in accordance with this procedure and appropriate updates made.

**On violations of this policy, management may take appropriate disciplinary action.**





## Continual Improvement Process

Document No. GIPCL/ISMS/PR/06

Release Date: 23<sup>rd</sup> May 2020

# Continual Improvement Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2 style="margin: 0;">Continual Improvement Process</h2>	Document No. GIPCL/ISMS/PR/06
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



## Continual Improvement Process

Document No. GIPCL/ISMS/PR/06

Release Date: 23<sup>rd</sup> May 2020

### Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Policy.....	4
4	Continual Improvement Process.....	6
4.1	Process Diagram .....	6
5	Identifying Improvements .....	7
6	Evaluation .....	7
7	Approval and Prioritisation .....	7
8	Management and Review.....	8



# Continual Improvement Process

Document No. GIPCL/ISMS/PR/06

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This policy covers the scope for the application of continuous improvement (CI) to the process.

## 2 Purpose

This document describes the way in which improvements will be identified, logged and managed to resolution.

## 3 Policy

### General guideline

This process is about identifying areas in which the ISMS could be improved and ensuring that these issues and ideas are logged, evaluated, actioned and reviewed in a coherent way.

The process as defined here assumes that you have a change management process in place and that improvements are managed through that. For larger changes a project will be initiated and the relevant documents created as part of that process (such as business case and project initiation document).

In general [Organisation name] will use the Plan-Do-Check-Act method (the Deming Cycle) for managing ISMS improvements as depicted below.



This is driven by the ISMS Policy which is updated on an annual basis and improvement objectives are set based on requirements of customers and the following inputs:



## Continual Improvement Process

Document No. GIPCL/ISMS/PR/06

Release Date: 23<sup>rd</sup> May 2020

- Information security policy
- Information security objectives
- Audit results
- Analysis of monitored events
- Corrective and preventive actions
- Management review

On-going success against these objectives is reviewed at quarterly management meetings and any action taken to ensure that [Organisation Name] is on track to achieving them.



## 4 Continual Improvement Process

### 4.1 Process Diagram

The process for identifying and achieving improvements is summarised in the diagram below.

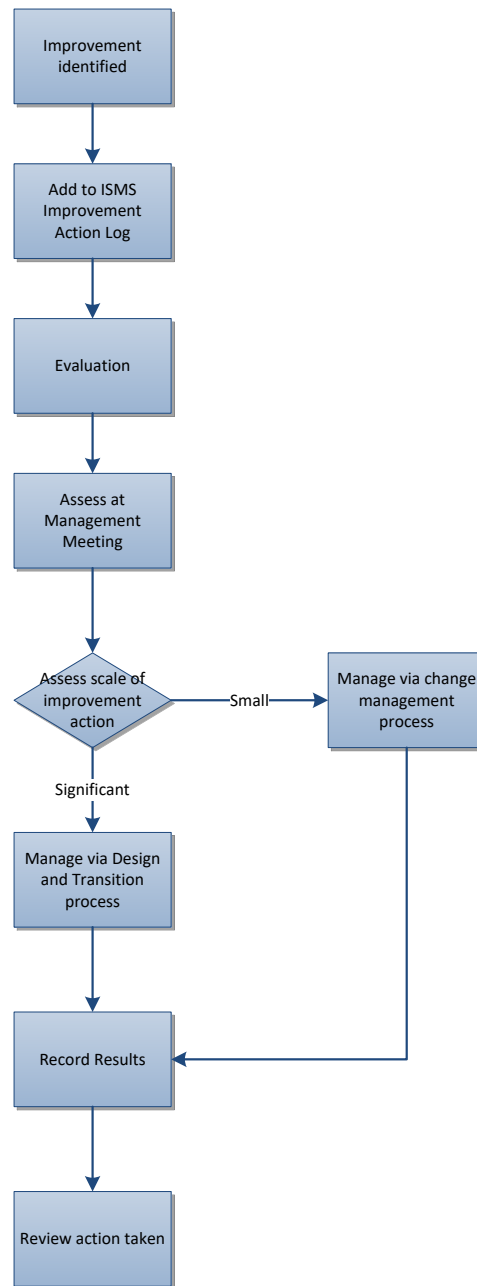


Figure 1 - Continual Improvement Process

	<b>Continual Improvement Process</b>	Document No. GIPCL/ISMS/PR/06
		Release Date: 23 <sup>rd</sup> May 2020

The detail of the above steps is described in the following sections.

## 5 Identifying Improvements

Improvements may be identified from any source and the [Information Security Manager] will encourage staff, users, customers and suppliers to propose ways in which they can be found. Such improvements may be identified from:

- Security reviews
- Team meetings
- Supplier meetings
- Risk assessments
- User surveys
- Internal and external audits

However, the above is not an exhaustive list.

Once identified, the improvement will be documented within ISMS10003 ISMS Improvement Action Log with a status of “Logged”. At this stage the action to achieve the improvement has not necessarily been determined. As much detail as possible should be specified as to the exact nature of the proposal.

## 6 Evaluation

Once logged, the improvement will be evaluated by the manager responsible for Continual Improvement to assess its importance and potential benefit and what needs to be done to achieve it. Other parties may be consulted during this stage to understand both the background and the implications and mechanics of making it happen.

## 7 Approval and Prioritisation

Once the improvement has been successfully identified it must be determined whether there is sufficient resource to implement it. The expected benefits of the improvement will also be documented in measurable terms where possible.

If the improvement is approved its status is changed to “Approved”.

The improvement action will now be prioritised against the others on the list to determine the relative allocation of resources and the likely timeframe of it. A scale of High, Medium and Low is used.



## Continual Improvement Process

Document No. GIPCL/ISMS/PR/06

Release Date: 23<sup>rd</sup> May 2020

### 8 Management and Review

Approved improvements will be managed and actions recorded via the ISMS Improvement Action Log and reviewed on a quarterly basis. Where the improvement requires a configuration item to be changed, a change request will be raised and the action will be performed under the control of the change management process. The change request number will be recorded against the ISMS improvement record in the ISMS Improvement Action Log.

For major changes the ISMS improvement process will interface with the Design and Transition of a New or Changed Service process which will ensure the improvement project is managed effectively.

Improvements will be categorised according to the area of the Information Security Management System they impact and reports produced on the number raised, approved and successfully implemented.

Once implemented, the effect of the improvement will be evaluated against the expected impact. If the benefits expected are not achieved, the reasons for this will be investigated as part of the regular review meeting.

**On violations of this policy, management may take appropriate disciplinary action.**





## Data Security Process

Document No. GIPCL/PR/07

Release Date: 23<sup>rd</sup> May 2020

# Data Security Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard	ISO/IEC 27001:2013
Version No.	1.0
Release Date	23 <sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujarat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Data Security Process</h2>	Document No. GIPCL/PR/07
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



## Data Security Process

Document No. GIPCL/PR/07

Release Date: 23<sup>rd</sup> May 2020

### Table of Contents

1	Scope .....	4
2	Purpose.....	4
3	Policy.....	4
3.1	Data at Rest.....	4
3.2	Data at Use.....	5
3.3	Data in Motion .....	5
4	Best practices for data Protection.....	5



# Data Security Process

Document No. GIPCL/PR/07

Release Date: 23<sup>rd</sup> May 2020

## 1 Scope

This policy covers all Sensitive business data Corporate trade secrets, national security information, personal medical records, Social Security and credit card numbers are all stored, used, and transmitted online and through connected devices.

## 2 Purpose

The Purpose of this process is to provide the data security in the organization and protection of data moving from one location to another across the internet.

## 3 Policy

### General guideline

Data Needs to be secured in three states and Each state presents unique security challenges.

- Data at Rest
- Data in use
- Data in Motion

### 3.1 Data at Rest

Data at rest is vulnerable to manipulation and its confidentiality, integrity, availability (CIA) must be protected. Data is stored on a hard drive it is data at rest. Information is primarily protected perimeter-based defences such as firewalls and antivirus programs. Organizations need additional layers of defences to protect sensitive data. Encrypting hard drives is one of the best ways to ensure the security of data at rest.

There are three best method to protect from unauthorized are as follows:

#### 1. Encryption

Data encryption, which prevents data visibility in the event of its unauthorized access or theft, is commonly used to protect data in motion and increasingly promoted for protecting data at rest.

The encryption of data at rest should only include strong encryption methods such as AES or RSA.



## Data Security Process

Document No. GIPCL/PR/07

Release Date: 23<sup>rd</sup> May 2020

## 2.Tokenization

Tokenization is a non-mathematical approach to protecting data at rest that replaces sensitive data with non-sensitive substitutes, referred to as tokens, which have no extrinsic or exploitable meaning or value.

Tokens require significantly less computational resources to process and less storage space in databases than traditionally encrypted data.

### 3.2 Data at Use

Data in use data must be access to thosed who need it, the more people and devices that have access to the data as per access the data also possibilities of greater risk the information it will end up in the wrong hands at some point. Organization use keys to securing the access of data and it is contol by the used by different type of authentication.

Organizations also need to be able to track and report relevant information so they can detect suspicious activity, diagnose potential threats, and proactively improve security.

### 3.3 Data in Motion

Organizations uses many services like faxes and conventional mails and all the growing volume of sensitive data be transmitted digitally so our data is most vulnerable when it is in motion. The best way to secure our messages organizations follow the users should be able to send and receive encrypted messages directly from their standard email service.

## 4 Best practices for data Protection

Best practices for robust data protection for data in transit and data at rest include:

1. Network security solutions like firewalls and network access control will help secure the networks used to transmit data against malware attacks or intrusions.
2. Don't rely on reactive security to protect your valuable company data. Instead, use proactive security measures that identify at-risk data and implement effective data protection for data in transit and at rest.
3. Choose data protection solutions with policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit.



## Data Security Process

Document No. GIPCL/PR/07

Release Date: 23<sup>rd</sup> May 2020

4. The best way to secure data in use is to restrict access by user role, limiting system access to only those who need it. Even better would be to get more granular and restrict access to the data itself.



## Vulnerability Management Process

Document No. GIPCL/PR/08

Release Date: 23<sup>rd</sup> May 2020

# Vulnerability Management Process



This document is the property of  
Gujarat Industries Power Co. Ltd.

Based on Reference Standard

ISO/IEC 27001:2013

Version No.

1.0

Release Date

23<sup>rd</sup> May 2020

Gujarat Industries Power Co. Ltd.  
P.O. Petrochemical, Vadodara, Gujrat -391346  
Tele: +91 265 2232768  
Fax: +91 265 2230029  
Website: <http://www.gipcl.com>

	<h2>Vulnerability Management Process</h2>	Document No. GIPCL/PR/08
		Release Date: 23 <sup>rd</sup> May 2020

### Document Release History

SN	Version No.	Release Date	Prepared By	Reviewed By	Approved By	Reasons for the Release
1	1.0	23 May 2020	Arnav Shukla	D B Jaani	Col S B Gurkha	Base line Initial Release



## Table of Contents

1	Purpose .....	4
2	Scope .....	4
3	Vulnerability Assessment Procedure.....	4
3.1	Scope Definition .....	4
3.2	Prerequisites.....	5
3.3	Timing and Scheduling.....	5
3.4	Procedure Steps.....	5
3.4.1	Reconnaissance .....	6
3.4.2	External Scanning.....	6
3.4.3	Internal Scanning .....	7
3.4.4	Reporting .....	7
3.5	Error Handling.....	7
3.6	Support and Escalation .....	8
3.7	Auditing and Logging .....	8
3.8	Monitoring.....	8

	<h1>Vulnerability Management Process</h1>	Document No. GIPCL/PR/08
		Release Date: 23 <sup>rd</sup> May 2020

## 1 Purpose

This document sets out a procedure to be used to assess technical vulnerabilities within the IT environment. Its intended audience is IT and information security management and support staff who will implement and maintain the organisation's defences.

## 2 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GIPCL business or interact with internal networks and business systems, whether owned or leased by GIPCL, the employee, or a third party.

This policy applies to employees, contractors, consultants, temporaries, and other workers at GIPCL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by GIPCL.

## 3 Vulnerability Assessment Procedure

This procedure is intended to be used by a suitably qualified specialist with a specific brief to assess a defined scope of systems and networks. It must only be used where the written permission of the owner of the systems and networks to be assessed has been obtained. If there is any doubt about this, the procedure should not be performed and clarification should be sought.

### 3.1 Scope Definition

The scope of the vulnerability assessment should be documented in as much detail as possible. According to the areas covered, this detail should include as a minimum:

- External assessment
  - external IP addresses included
  - external IP addresses specifically excluded
  - Websites included
- Internal Assessment
  - Names of servers included
  - IP address ranges included
  - IP addresses specifically excluded
  - User computers to be assessed

The agreed scope should be signed off by [Information Security Manager] and [Service Manager].

### 3.2 Prerequisites

Before starting the assessment the following prerequisites must be in place:

- The assessment scope is fully defined
- Written permission is provided for the defined scope
- Assessors are adequately trained on the tools to be used and the vulnerability assessment process
- Service managers of the systems to be assessed have been informed of the purpose and timing of the exercise
- The tools to be used are installed and fully updated

The vulnerability assessment will be carried out using the following set of tools:

Tool Name	Supplier	Purpose
Kali Linux	Offensive Security	Assessment platform
nmap	Open source	Network scanning
Nessus	Tenable	Vulnerability scanning
NeXpose	Rapid 7	Vulnerability scanning
HTTRACK	Open source	Website copying
The Harvester	Open source	Web reconnaissance
Whois	Open source	Web reconnaissance
nslookup	Open source	DNS reconnaissance

These tools should be installed on a computer which has itself been tested for vulnerabilities and is subject to full security protection (e.g. anti-virus, firewall) as per GIPCL policies. Detail regarding how to use these tools is not provided in this procedure.

### 3.3 Timing and Scheduling

In general it is desirable to run the scanning aspects of this procedure out of normal business hours although this may be relaxed with the prior agreement of management.

### 3.4 Procedure Steps

The procedure consists of the following steps:

1. Reconnaissance
2. External Scanning
3. Internal Scanning

	<h2>Vulnerability Management Process</h2>	<p>Document No. GIPCL/PR/08</p> <hr/> <p>Release Date: 23<sup>rd</sup> May 2020</p>
-----------------------------------------------------------------------------------	-------------------------------------------	-------------------------------------------------------------------------------------

#### 4. Reporting

Once the initial reconnaissance stage has been completed scanning for vulnerabilities can be carried out. This will be in two stages:

- External scanning of the network perimeter from outside the organisation network
- Internal scanning of specific networks, servers and clients from within the network perimeter

Both types of scan are required in order to assess vulnerabilities from external and internal threats. A full report will then be produced.

These steps are described in more detail below. Note that the procedure does not include the use of exploitation tools to test whether an identified vulnerability can in fact be exploited successfully. Due to the potential to disrupt business operations, this type of invasive penetration testing must only be carried out by qualified and experienced specialists at the specific request of senior management.

##### 3.4.1 Reconnaissance

The first step of the assessment will be to perform reconnaissance activities via the Internet to determine the type and amount of information about the organisation freely available to an attacker.

##### 3.4.2 External Scanning

Scanning for vulnerabilities in the outward-facing perimeter of GIPCL network must be carried out from a computer connected directly to the Internet and not connected to the internal network.

Using the information provided and that gathered as part of the reconnaissance stage, assess what can be determined about the network from outside. This can be done using the nmap tool in its command line form or one of the GUI front ends to nmap such as Zenmap. Make sure that only the IP addresses within scope are scanned.

A picture should be built up of the visible hosts, their names, IP addresses, open ports and services.

From this picture, use the Tenable Nessus Vulnerability Scanner to run a scan using an appropriate policy against the targets identified. Make sure you update the plug-ins before running the scans. Record the results of the scan, including warnings and vulnerabilities found.

### 3.4.3 Internal Scanning

In order to run an internal scan you will need to use a computer that is connected to the internal network and has access to the hosts and networks that need to be scanned. Run an nmap scan within the subnet to ensure that the target computers are reachable.

Use the Tenable Nessus Vulnerability Scanner to run a scan using an appropriate policy against the targets that are defined to be within the scope of the exercise. Make sure you update the plug-ins before running the scans. Record the results of the scan, including warnings and vulnerabilities found.

### 3.4.4 Reporting

From the information collected as part of the reconnaissance, external scanning and internal scanning stages, a report should be produced which clearly sets out the vulnerabilities found and their severity.

The report should include:

- Management Summary
- Assessment Scope
- Methods and tools used
- Results
- Conclusions
- Prioritised action plan

The classification of the report should be “Restricted” and should be provided to the sponsor of the assessment only. Technical detail should be included as appendices in order to improve readability.

## 3.5 Error Handling

The following common errors may occur during this procedure:

Stage of Procedure	Error	Possible Cause	Recommended Action
External Scanning	IP address given is not correct	Reboot of router may have caused a new IP address to have been assigned via DHCP	Obtain new IP address; ensure router is not rebooted
Internal Scanning	Host to be tested is not reachable	Host is on a different VLAN to the testing computer	Connect testing computer to correct VLAN

### 3.6 Support and Escalation

If an error occurs which cannot be corrected using this procedure, support should be obtained using the following information:

Support Person	Role	Phone Number	Hours of availability
xxx	Senior Vulnerability Assessor	Xxx xxx xxxx	09:00 to 17:30 Monday to Friday
Tenable support desk	Nessus support	Xxx xxx xxxx	09:00 to 17:30 Monday to Friday

### 3.7 Auditing and Logging

Records should be kept of all activities carried out as part of the vulnerability assessment, including names, dates and times.

### 3.8 Monitoring

All scans should be monitored in real time. Scans should not be left to run unattended overnight or over a weekend or scheduled at such times.