
	Information Systems	Internal
		GPIL / IS / Cyber Policy / new
		Revision No: 01
CR-CDR-M-012	Cyber Security Policy	Issue Date: 25-Sep-2020
		Effective Date: 01-Oct-2020

Revision History Sheet

Ref. Document	Associate Document	Rev. Date	Rev. No.	Reason for Change	Initiated By	Approved By
Cyber Security Policy	NA	Nill	00	Document Numbering Scheme	Functional Team Lead	Functional Head IS
Cyber Security Policy	NA	30.09.2022	01	Revision	Functional Team Lead	Functional Head IS

	Information Systems	Internal
		GPIIL / IS / Cyber Policy / new
CR-CDR-M-012	Cyber Security Policy	Revision No: 01
		Issue Date: 25-Sep-2020
		Effective Date: 01-Oct-2020

Introduction

In a technology driven world the internet is its bloodline. We heavily rely on internet technology to transact business , which makes us more vulnerable to security breaches. Sources of such breaches/attacks may vary such as human errors, hackers and system & network malfunctions, causing damages both tangible and intangible like financial or production loss or goodwill of Genus.

To address such concerns, we must implement necessary cyber security measures with detailed instructions in risk mitigation.

Objective

This policy will provide guidelines and provisions for securing Information assets and infrastructure in advent of any Cyber security event.

Scope

This policy applies to all of Genus's employees, vendors/contractors, and anyone else who may have any type of permanent or temporary access to Genus's systems software and hardware , applicable for all locations

SECURITY GUIDELINES

Confidential data


Following data set is organization's secret and are valuable and considered as classified and confidential

- ❖ Unpublished financial information
- ❖ Tendering details
- ❖ Data of customers/partners/vendors
- ❖ Design Documents
- ❖ Bill of Materials
- ❖ Product Costing
- ❖ Technical datasheets, Patents, formulas or new technologies
- ❖ Client list (existing and prospective)
- ❖ Employee/Users Data
- ❖ SAP Financial /Purchase Report Data.

All employees are obliged to protect the above mentioned data.

Users Guideline

- ❖ Users shall not share the PC and Network configuration details with any other user or an outsider.
- ❖ Changing the basic configuration, or installation of any hardware / software by user is prohibited without written permission from IS .
- ❖ Attempt to gain access to any other computer on the Network (with or without using specialized software / hardware for this purpose) is restricted unless and otherwise permission obtained from IS
- ❖ Users shall not change any Antivirus configuration as implemented by IS dept
- ❖ Users must be careful and take all responsibility while allowing anyone (internal or external) to use

	Information Systems	Internal
		GPIIL / IS / Cyber Policy / new
CR-CDR-M-012	Cyber Security Policy	Revision No: 01
		Issue Date: 25-Sep-2020
		Effective Date: 01-Oct-2020

devices / access credentials (like user name , password etc) allotted to him / her .

Users shall

- ❖ Ensure that the system is protected with Domain Login Password
- ❖ No Files or Folders shall be shared over the network except for FTP / Print Sharing. All files and folders should be stored and shared using G-Drive.
- ❖ Ensure that PC / Laptop is installed with the latest version of AV patches and virus definitions.
- ❖ Ensure that latest patches for Operating System are applied on their PC / Laptop

NETWORK SECURITY

- ❖ Use of the Network for illegal activities, including using it against the company you belong to in particular, and the GENUS in general, is **strictly prohibited**
- ❖ Deliberate attempts to disrupt the performance of the Network or any other computer system / network, shall attract severe action against such user
- ❖ Users are prohibited to make changes in network connection mode (**PC / Laptop users MUST NOT USE Wireless and Wired Connection together**)
- ❖ Any external devices belonging to outsiders will not be allowed to access any internal information asset over internal network

EMAIL SECURITY

Emails are being used by hackers using new and sophisticated methods to attack systems and data thefts both personal and corporate. We recommend following best practices to all employees to follow completely:


- ❖ Unsolicited mails must not be opened however tempting it may be.
- ❖ Must avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- ❖ Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- ❖ Check email and names of people they received a message from to ensure they are legitimate.
- ❖ Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they can refer to the IT Team.

Data Security

Data transfer is one of the biggest sources of security risk. Most of the virus attacks’ reason can be traced back to use of external media such as pen drives. All employees must follow following steps to avoid:

- ❖ Business data is classified and access is restricted to individuals responsible using authorization controls (e.g. SAP data access is controlled by user Role or profile based).
- ❖ Unstructured data content like files, spreadsheets, etc shall be stored on G-Drive with proper access control. Sharing of such data shall be the sole responsibility of the individual.
- ❖ The recipients of the data should be properly authorized people or organizations and have adequate security policies.

	Information Systems	Internal
		GPIL / IS / Cyber Policy / new
CR-CDR-M-012	Cyber Security Policy	Revision No: 01
		Issue Date: 25-Sep-2020
		Effective Date: 01-Oct-2020

- ❖ Any suspicious activities, scams, privacy breaches and hacking attempts must be reported to the IS team on priority.
- ❖ Individuals shall be responsible for archiving their important data with help of IS from time to time.

INTERNET SECURITY / USAGE

The Internet is the bloodline of business in present times and people and businesses are relying on the internet for their success and is part of their growth strategy. But, it has its inherent security threats which is a big concern. To allay this, we at Genus take pride in our Internet Usage Policy adherence to which will assure the protection from risks emerging due to internet usage.

- ❖ Copyright Violation
- ❖ Offensive language
- ❖ Confidentiality
- ❖ Unauthorized use
- ❖ Social Media Platforms
- ❖ E-commerce Websites


Password Guidelines

A Strong and unique password is a prerequisite for having the basics of security right. We at Genus encourage users to follow basic guidelines mentioned in the Password Management Policy. Some of them is outlined below:

- Use hard-to-guess passwords or passphrases. A password should have a minimum of 8-10 characters using uppercase letters, lowercase letters, numbers and special characters.
- Use different passwords for different accounts.
- Keep your passwords or passphrases confidential.

ENFORCEMENT

- ❖ In case of any security breach, the matter needs to be immediately reported to the Local IS Head along with Local HR & Admin.
- ❖ Parallely , the matter may be reported to the Corporate IS Head for further escalation, if needed.

	Information Systems	Internal
		GPIIL / IS / Cyber Policy / new
		Revision No: 01
CR-CDR-M-012	Cyber Security Policy	Issue Date: 25-Sep-2020
		Effective Date: 01-Oct-2020

Disciplinary Action

We at Genus expect employees to behave with responsibility and always follow this policy. Any non-compliance/non-adherence causing damage to organization's interest will attract disciplinary action:

Non-compliance Type	Impact	Action *
First-time, unintentional, small-scale security breach	Limited Impact, Containment non-critical	A verbal warning and training the employee on security
Intentional, repeated, small-scale security breach	Regional Impact, Containment critical, In-house Action	A warning letter will be issued and a penalty will be levied.
Intentional, repeated or large scale breaches severe financial or other damage	Wide Impact, Containment critical, External resources required.	Matter will be suitably escalated to competent authority / management for disciplinary action

* Management will examine each incident on a case-by-case basis and have final say in such matters.