E. I. D.-Parry (India) Limited

Cyber Security Policy

Adoption date and Effective Date : April 01, 2022

CYBER SECURITY POLICY

1. *Preamble*

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks. In the light of the growth of IT in the sphere of business, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the need of the hour. The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users.

2. *Purpose:*

The purpose of the policy is to protect information and information infrastructure from cyber incidents through a combination of processes, guidelines, technology and cooperation. This policy governs the usage of IT Resources from an end user's perspective.

This Policy defines what we want to protect and what we expect of our system users. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords and describes how we will monitor the effectiveness of our security measures.

3. *Scope and Applicability:*

This policy applies to EID Parry including its Associate Companies, Subsidiaries, and Joint Venture. EID Parry also expects independent contractors and all involved in the value chain to uphold the principles of this Policy and urges them to adopt similar policies within their own businesses. It is mandatory for all users to adhere to the provisions of this policy.

4. *Effective date:*

This Policy shall come into force on 1st April 2022 .

5. *Policy Statement*

- The Company will protect all its stakeholders' interests by ensuring confidentiality, Integrity and continuous availability of information and information systems under its control which includes, but is not limited to electronic, print information etc., on servers, workstations, laptops, networking and communication devices, tapes, CDs, and information printed or written on paper or transmitted by any medium.

- The Company is committed to comply with all legal, regulatory, and contractual security obligations as may be applicable in cyberspace.

- The Company shall evaluate the business risk in information security perspective, prevent and reduce the risks to the maximum possible extent to avoid any undesired effects on business and Customers

- The Company shall protect all Information from unauthorized access, use, disclosure, modification, disposal, or impairment whether intentional or unintentional, through appropriate technical and organizational security measures

- The Company is committed to provide a virus free network and all Information processing systems will be auto updated with latest security patches from the manufacturer and loaded with an approved antivirus system.

- The Company shall provide framework to manage and handle security breaches, violations and business disruptions.

- The Company shall ensure continuity of critical operations in line with business and contractual requirements.

- A comprehensive backup procedure will be implemented to protect the business transactions. Backup tapes are to be verified by restoring the data for integrity as per SOP.

- Only authorized and licensed software will be allowed to be installed on corporate systems.

- Company network will be always protected from the Internet through a firewall.

- All third-party partners dealing with the Company who use IT information assets will be asked to sign a non-Disclosure agreement (NDA)

- All servers to be located in a secured area with restricted access.

- All information assets used in production will have either warranty or a support contract from the authorized vendor/ partner

- Disposal of media, any information processing systems will follow the E-waste policy.

- All changes in the information processing system will be managed through the change control process

6. *Policy - Concepts & Guideline*

i. Confidentiality

The assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality is critical to total data security. Encrypting data by using digital certificates and Secure Socket Layer (SSL) or virtual private network (VPN) connection helps ensure confidentiality when transmitting data across untrusted networks.

ii. Auditing security activities

Monitoring security-relevant events to provide a log of both successful and unsuccessful (denied) access. Successful access records tells who is doing what on your systems. Unsuccessful (denied) access records tells either that someone is attempting to break your security or that someone is having difficulty accessing your system.

iii. Authentication of Access:

All devices on the network of E.I.D.-Parry (India) Limited ("Company") should not be accessible without proper authentication. Authentication for access of the Company's computer networks shall be obtained after following the due process and procedure as prescribed by the IT team.

The assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access a system. Traditionally, systems have used passwords and user names for authentication; digital certificates can provide a more secure method of authentication while offering other security benefits as well. When system is linked to a public network like the Internet, user authentication takes on new dimensions. An important difference between the Internet and intranet is the ability to trust the identity of a user who signs on. Consequently, one should consider seriously the idea of using stronger authentication methods than traditional user name and password logon procedures provide. Authenticated users might have different types of permissions based on their authorization levels.

iv. Authorization:

Authorization implies assurance that the person/computer at the other end of the session has permission to carry out the access authentication request.

Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Typically, authorization is performed in context of authentication.

v. Integrity:

Integrity would imply the assurance that the arriving information is the same as what was sent out. Understanding integrity requires to understand the concepts of data integrity and system integrity.

a) Data integrity: Data is protected from unauthorized changes or tampering. Data integrity defends against the security risk of manipulation, in which someone intercepts and changes information to which he or she is not authorized. In addition to protecting data that is stored within our network, we might need additional security to ensure data

integrity when data enters our system from untrusted sources. When data that enters our system comes from a public network, we need security methods so that we can perform the following tasks: –

- Protect the data from being sniffed and interpreted, typically by encrypting it.
- Ensure that the transmission has not been altered (data integrity).
- Prove that the transmission occurred (nonrepudiation). In the future, you might need the electronic equivalent of registered or certified mail.

b) System integrity: Our system provides consistent and expected results with expected performance. For the OS operating system, system integrity is the most commonly overlooked component of security because it is a fundamental part of OS architecture.

vi. Security Incident Management Process:

a) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of data owned by the Company.

b) IT Department reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of the system.

vii. Use of IT Devices:

IT devices (Desktops, Printers, Scanners, Standalone PCs and other electronic devices connected to our network) issued by the Company to a user should be primarily used for official purposes and in a lawful and ethical manner.

viii. E-mail Access from the Company's Network:

a) E-mail service authorized by the Company should only be used for official correspondence.
b) All incoming SMTP e-mails will be scanned for spam and virus infection.

ix. Access to Social Media Sites from the Company's Network:

a) Use of social networking sites by employees is governed by the IT Department. User should comply with all the applicable provisions under this policy while posting any data pertaining to the Company on social networking sites.

b) User should adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, discrimination, harassment and other applicable laws.

c) User should report any suspicious incident as soon as possible to the IT Department.

d) User should always use high security settings on social networking sites.

e) User should not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

f) User should not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.

g) User should not make any comment or post any material that might otherwise cause damage to the organization's reputation.

x. Filtering and blocking of sites:

a) IT Department may block content over the Internet which is in contravention of this policy and other applicable laws of the land in force which may pose a security threat to the network.
b) IT Department may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.

XI. The following Policies and Guidelines will also cover under this Policy:

a) Policy and Guidelines on the Use of IT Resources: This governs the usage of IT Resources from an end user's perspective. Guidelines supports the implementation of this policy by providing the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners.
b) E-mail Policy: This governs the usage of email services provided to employees.
c) Password Policy: 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 of passwords.
d) Policy on Adoption of Open-Source Software. This will encourage the formal adoption and use of Open-Source Software (OSS)
e) Backup Policy for Servers: The purpose of this policy is to provide consistent rules for backup management to ensure backups are available when needed.

7. *<u>Policy Compliance and Dissemination</u>*

a) It is the responsibility of all employees to adhere to the policy and the management has all rights to take disciplinary action in case of its violation.
b) All employees of the organization are necessarily to be aware of the Information Security Policy of the organization.
c) Employees while operating from remote/outside organization network should strictly connect via VPN for accessing Applications and Corporate Network.
d) All employees should implement appropriate controls to ensure compliance with this policy by their users.
e) IT Department will ensure resolution of all incidents related to the security aspects of this policy by their users.

f) Users should not install any network/security device on the network without consultation with the Implementing Department

g) The IT Department should ensure that training and awareness programs on use of IT resources are organized at regular intervals. To ensure security awareness amongst Employee to enable them to meet their security obligations. It Department should ensure proper dissemination of this policy. IT Department may use newsletters, banners, bulletin boards, corporate Websites and Intranet etc. to increase awareness about this policy amongst their users.

h) Orientation programs for new recruits should include a session on this policy.

8. *Monitoring and Review:*

The Company shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy. The Company for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc. Monitoring and review of this policy is governed by IT department. A periodic reporting mechanism to ensure the compliance of this policy should be established by the IT Department.

Any security incidents, security weaknesses and infringement of the policy actual or Suspected, are reported, investigated by the designated SOC team and appropriate corrective and preventive action initiated.

The Managing Director in consultation with the IT- Head is authorized to make modifications to this policy as and when deemed necessary and appropriate to ensure the ends of the policy being served.

9. *Reporting and Remedy:*

Any questions or concerns on matters concerning Cyber Security shall be reported to IT-Head, Corporate.

EID Parry assures through this policy that any Cyber Security Matters resulting from or caused by the Company's business activities shall be appropriately and adequately remedied in a time-bound manner.