DEEVEE COMMERCIALS LIMITED

Information Security Policy

1. Introduction

1. This Policy Document encircles all aspects of security surrounding confidential company information and its protection in order to achieve organizational goals. This policy must be distributed amongst all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understood this policy fully.

2. The Company shall observe the International Standards Organization (ISO), wherever feasible, to adopt best practices, which are widely acceptable and reliable.

2. Purpose

The policy provides the security foundation necessary to protect the company's Information Assets by:

1. Establishing an **information security architecture** for standard security controls;
2. Defining **organizational roles and responsibilities** for information security;
3. **Developing and reviewing** the Information Security Policy;
4. Monitoring and measuring the **implementation** of the Information Security Policy; and
5. Developing and delivering a **program to maintain** information security **awareness.**

3. Roles and Responsibilities

1. **Management** – The Board of Directors of the Company, or such other authority as may be designated by the Board, must have in place a framework which would provide adequate safeguards to protect sensitive information, ensuring compliance with various regulations and to guard the future of the organization.

2. Chief Security Officer –

   a) The Chief Security Officer (CSO) (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to the following:

      (1) Creating and distributing security policies and procedures. It is required that all employees confirm that they understand the content of this security policy document.

      (2) Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.

      (3) Creating and distributing security incident response and escalation procedures that would include maintaining a formal security awareness program for all employees.

DEEVEE COMMERCIALS LIMITED KOLKATA

b) The CSO shall be appointed by the Board of Directors of the Company or such other authority as may be designated by the Board and all the team members/ employees subordinate to CSO will be appointed by the Human Resources Office in consultation with the CSO;

c) The CSO shall have adequate number of team members under him, to ensure adequate efficiency and effectiveness in performance of the tasks. The employees reporting to CSO must possess all the skills required to perform their tasks well and the CSO must have access to such tools and techniques which help in establishing security systems in the Company;

d) There should be clear segregation between the role of CSO and the IT division, to ensure confidentiality of data and integrity in process flow. This must clearly be defined in the terms of appointment of CSO and the employees in the IT division.

3. **Information Technology Officer** - The Information Technology Officer (or Chief Technology Officer or equivalent) is an officer who is primarily responsible for the development and implementation of information technology systems in the organization and who is designated as such by the Board or the senior management of the Company. He must work in consonant with the CSO and any matter which may have a material bearing on the security and IT functions of the Company, must be immediately reported to CSO by him. He shall conduct daily administrative and technical operational security procedures (for example, user account maintenance procedures, and log review procedures).

4. **System and Application Administrators** – System and Application Administrators will be primarily responsible for continuous operation of information technology systems of the organization. The ITO shall be responsible for appointing or designating such number of persons as System and Application Administrators, as it deems fit. They shall ensure that the all the IT resources of the organization are intact and performing efficiently. They shall:

a) monitor and analyse security alerts, information and distribute them to appropriate personnel;

b) administer user accounts and manage authentication;

c) monitor and control all access to data;

d) maintain a list of service providers;

e) ensure there is a process for engaging service providers including proper due diligence prior to engagement.

5. **Human Resources Office** – Apart from other functions carried out by it, the Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program and ensure the following:

a) that the awareness programs are facilitated at least once annually.
b) that the employees acknowledge in writing at least annually that they have read and understand the Company's information security policy;
c) that the written contracts with service providers adhere to PCI-DSS;
d) that the written contracts with service providers include acknowledgement or responsibility for the security of data by the service provider.

6. **User Manager** – User Manager(s) shall be responsible to ensure continuous support services to the user. Their role would be to primarily act as an interface through which users can interact and place any requests. A user manager usually shall have access/ right to modify or change user profile and related data.

7. **Other General Roles and Responsibilities of Employees** - Employees handling sensitive data should:

a) Handle Company's & clients' information in a manner that fits with their sensitivity;
b) Once confidential data has been entered, its integrity and privacy must be protected on the databases and servers where it resides;
c) The information data must be available to the users and should be protected against loss of use to ensure uninterrupted flow of business operations;
d) The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
e) Use of e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal is strictly prohibited;
f) Do not disclose personnel information unless authorised;
g) Keep passwords and accounts secure;
h) Prior approval from management to be obtained to install/ establish any new software or hardware, third party connections, etc.;
i) Always leave desks clear of sensitive data and lock computer screens when unattended by pressing the window key along with letter 'L';
j) Employees should ensure that technologies should be used and setup in acceptable network locations.
k) All PCs, laptops and workstations should be secured with a password-protected screen saver with the automatic activation feature.
l) All Point of Service (POS) and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
m) Since information contained on portable computers is especially vulnerable, special care should be exercised in there usage.
n) Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own

and not necessarily those of the Company, unless posting is in the course of conducting business duties.

o) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Identification and Classification of Information Assets

1. "Information Asset" is a collective body of information, stored in any manner and recognized as having value for the purpose of enabling an agency to perform its business functions, thereby satisfying a recognized agency requirement.
2. The primary responsibility of identification and classification of Information Assets rests with the CSO. He may delegate the process to his subordinates which may sub-delegate the same to junior level employees. Since, this is a continuous process, reporting must be done through the chain of command.
3. A detailed inventory of Information Asset with distinct and clear identification of the asset must be documented and maintained in the following manner –
   a) Identification of assets;
   b) Documenting and maintaining asset inventories;
   c) Loss, theft or misappropriation of assets.
4. Information Assets can be classified in the following manner:
   a) Assets depicting similar nature must be grouped together under one classification. For e.g. All information related to credit should be classified as financial assets;
   b) Only those assets should be identified which possess value to the Company and add to further the business activities of the Company;
   c) Mere sources of information should not be confused to be Information Assets;
   d) Single data unit should not be considered as Information Asset;
   e) Classification should be recorded well, in terms of nature, name, brief description of the asset, value creation and areas affected, to name a few;
   f) Any information must be verified with its source before its classification and record-keeping.

5. Access Control Policy

1. Authority to access and usage of Information Assets and other IT processes should be clearly defined in the roles and responsibilities of terms of contract with each employee in the chain of command.
2. Access is allocated in terms of authority and chain of command and by means of a unique Active Directory account and complex password, and the password should not be changed unless directed by the CSO or any other authority delegated by CSO.
3. Access to confidential information should be restricted to the Management and CSO and ITO, unless otherwise is directed by them;

DEEJEE COMMERCIALS LIMITED KOLKATA

4. Administrative access including access adequate to perform execution tasks are appropriately provided to junior level employees based upon the use and their respective roles;
5. The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
6. Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
7. Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
8. Password issuing, strength requirements, changing and control will be managed through formal processes.
9. Users shall become familiar with and abide by the Company policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
10. Access for remote users shall be subject to authorization by IT services and be provided in accordance with this Policy. No uncontrolled external access shall be permitted to any network device or networked system.
11. Access control methods include logon access rights, Windows share and New Technology File System (NTFS) permissions, user account privileges, server and workstation access rights, firewall permissions, Internet Information Services (IIS) intranet/extranet authentication rights, Structured Query Language (SQL) database rights, isolated networks and other methods as necessary.
12. A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT services to review users' access rights. The review shall be logged and IT services shall sign off the review to give authority for users' continued access rights.

6. Personnel Security

1. Appropriate background checks (such as criminal and credit record checks, within the limits of the local law) must be performed. Appropriate credentials for facility personnel, with privileged access like System and Application administrator, and, as appropriate to protect the Company in the event of misuse of data or fraud before they commence their employment with the Company must be ensured.
2. Personnel using the devices should be trained about handling the POS devices. While using, they should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.

7. Physical Security

1. Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.
2. Personnel should ensure that they have appropriate credentials and are adequately authenticated for the use of technologies.
3. Personnel should ensure that technologies should be used and setup in acceptable network locations.
4. Personnel shall keep their passwords secure and not share private information of their accounts.

8. Maker-checker

1. The company shall automate controls by introducing a computer program with logical access, segregation of duties and maker/checker controls to minimize the chance of fraudulent payments. The user manager (Primary/Secondary) can play dual role as Maker/Checker.
2. However, maker cannot check/authorize the transactions made by him/her. User manager will have access to all the menus available to different users. This will reduce the risk of error and will ensure reliability of information.

9. Information Security Incident Management

1. Security incident is an event that may result in:

    a) degraded system integrity
    b) loss of system availability
    c) disclosure of confidential information
    d) disruption of activity
    e) financial loss
    f) legal action
    g) unauthorized access to applications
    h) loss of data

2. The Company shall observe ISO/IEC 27035-1:2016, in dealing with security incidents in the organization.
3. The company shall have the following responsibilities with respect to incident response:

    a) Work with the information security community to make recommendations for securing networks, systems, and applications.
    b) Educate CSO and end users on the goals and operations of the Company;

DEEVEE COMMERCIALS LIMITED ★ KOLKATA

c) Define the process by which the company responds to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities.

d) Provide a service level for the company's response to computer security incident reporting and advisories that are received from external organizations, that may have a potential impact on company's computer systems.

e) Promote computer security risk awareness so the personnel are better prepared to handle incidents.

f) Take actions to verify that an incident actually occurred upon learning of a potential incident and determine the scope and impact of each intrusion, to prioritize actions accordingly.

g) Once an incident is verified/ validated, its magnitude must be determined and an electronic log of each such incident must be maintained.

h) All the incidents as recorded must be reported to the office of CSO or the Management as such intervals as deemed necessary. Incidents which are critical and material in nature and which may affect the operations of the Company must be reported forthwith to the CSO.

i) Review of existing management system is required based on the incidents recorded, on a quarterly/half-yearly basis, to ensure that systems remain updated.

10. Audit and Log review

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification and shall form part of audit trails.

11. Policy Review

This Policy must be reviewed by the Board at such intervals as may be required.

DEEVEE COMMERCIALS LIMITED * KOLKATA