**Information Security Breach Policy**

Version: 1.0

**Document Key Information:**

|  |  |
| --- | --- |
| **Title:** | Information Security Breach Policy |
| **Topic:** | Information Security |
| **Classification:** | Policy |
| **Status:** | Draft |
| **Owner Department:** | Information Technology |
| **Document Approver:** | Board of Directors |
| **Group/Local Scope:** | [COMPANY NAME]  |
| **Version:** | 1.0 |
| **Last Review Date:** | December 2022 |
| **Next Review Date:** | December 2023 |

**Document Change Control:**

To track reviews, updates and approvals actions related to the document

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** | **Date:** | **Change Description Summary** | **Change by:** |
| 1.0 | 1.12.2022 | Initial Document | CISO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Introduction 4](#_Toc113540360)

[2. Purpose 4](#_Toc113540361)

[3. Policy Statement 4](#_Toc113540362)

[4. ISO 27001 Controls Addresses 5](#_Toc113540363)

[5. Disciplinary Action for Breaches of Security Policy 5](#_Toc113540364)

[6. Infringement Violation and Classification 6](#_Toc113540365)

[7. Workstations Usage User Agreement 7](#_Toc113540366)

[8. Non-Conformance 8](#_Toc113540367)

[9. Security Incident Reporting 8](#_Toc113540368)

[10. Information Security Violation Escalation 8](#_Toc113540369)

[11. Responsibilities 9](#_Toc113540370)

[12. Definitions 10](#_Toc113540371)

[13. Information Security Violation Escalation Procedure 11](#_Toc113540372)

[14. Information Security Violation Category 17](#_Toc113540373)

[15. Procedures for making Amendments to Policies 17](#_Toc113540374)

[16. Annexure 1: Information Security Violation Investigation Form 18](#_Toc113540375)

1. Introduction

Ensuring that [COMPANY NAME] information is protected from unauthorized disclosure and safeguarding to prevent unauthorized modification or destruction is an essential pre-requisite for implementing secure systems at [COMPANY NAME]. Such monitoring provides management with assurance that the Confidentiality, Integrity, and Availability of its Information resources will not be compromised. This policy will be enforced. Therefore, all [COMPANY NAME] employees, contractors, vendors, and temporary staff must acknowledge and comply with this policy.

The enforcement of this policy and all Information Security policies is important in delivering the message to all [COMPANY NAME] staff and all the respective outsourced parties that organizational security is a serious issue. Breach of confidentiality and any compromise of information or systems resources in respect of confidentiality, availability, and integrity is a punishable offense, requiring disciplinary action by both line Management and the Human Resources Division of [COMPANY NAME].

1. Purpose

This policy serves to ensure all [COMPANY NAME] employees and outsourced parties are aware of and are familiar with the stance the Management of the [COMPANY NAME] will take towards employees (permanent or other), who breach information security policies of [COMPANY NAME]. The action to be taken against the individual/group violating the policy shall be in consultation with the Human Resource Department.

This policy will form a part of the induction package for all new employees of [COMPANY NAME] and agreements with outsourced 3rd party suppliers.

1. Policy Statement

[COMPANY NAME] Management will enforce disciplinary action on all security breaches of its Information Security Policies.

All [COMPANY NAME] employees, contractors, vendors, and temporary staff must adhere to the Information Security Policies of [COMPANY NAME]. Every employee has an obligation and duty to appropriately protect the [COMPANY NAME] system resources and data, electronic or other media.

1. ISO 27001 Controls Addresses

A.15.1.1 – Identification of applicable legislation

A.7.1.3 – Acceptable use of assets

A.13.1.1 – Reporting information security events

1. Disciplinary Action for Breaches of Security Policy

Any identified infringement of security Policies will be escalated to Senior Management and the Human Resources (HR) for immediate disciplinary action. Enforce will be based on the infringement category.

[COMPANY NAME] – Executive Management will be a part of the process for disciplinary actions enforced by HR. These disciplinary actions could include permanent dismissal from the employment of [COMPANY NAME] / termination of the contract for outsourced parties for major violators of the [COMPANY NAME] Policies. Such disciplinary action may include (without limitation):

* Counselling
* Verbal or written warnings
* Denial of access to premises or systems
* Suspension from employment
* Dismissal / Termination of employment
* Summary dismissal
* Civil and / or legal proceedings according to the laws
1. Infringement Violation and Classification

|  |  |
| --- | --- |
| **Description of Violation**  | **Risk Ranking**  |
| Using another staff member’s password to gain access to any system under that other person’s Logon ID.  | **High Risk** The process for authentication and accountability holds whoever owns the access codes and ID accountable and responsible for any activity under that ID. If you knowingly give your ID and password to another staff member to use. Hence both the person using the ID and the person who gave the ID and password will be disciplined. (It is a different matter if somebody sees you type your password and then uses it to log onto a system without your prior knowledge.) **Disciplinary Procedure:** **Step 1.** HEAD OF IT to be informed by whoever identifies an infringement of Security Policies. **Step 2**. HEAD OF IT, to escalate to the Executive Management and Human Resources Division. **Step 3**. Executive Management and Human Resources Management to enforce disciplinary action.  |
| Attempting to run workstations software hacking tools on any [COMPANY NAME] resources. (Malicious intent like cardholder data theft)  | **High Risk** This is a most serious offense and is seen as a breach of the Information Security Policy.**Disciplinary Procedure:** **Step 1.** HEAD OF IT to be informed by whoever identifies an infringement of the Security Policies. **Step 2**. HEAD OF IT, to escalate to the Executive Management and the Human Resources Division. **Step 3**. Executive Management and Human Resources Management to enforce disciplinary action.  |
| Connecting to the [COMPANY NAME] Network and simultaneously connecting into the Internet, bypassing the Proxy, firewall.Using a Dial-up modem / USB internet sticks like Mifi/Mobile Hotspots connected to the internal network is not authorized. All Internet connections that are not stand-alone must go through the [COMPANY NAME] internal Proxy Server, and these connections must be pre-approved by IT department.  | **High Risk** This is a most serious offense and is seen as a breach of the Information Security Policy.**Disciplinary Procedure:** Same as above  |
| Loading/installing unlicensed software or pirated software onto any workstations/server.  | **Medium Risk** This is an in-direct violation of the [COMPANY NAME] Security Policies. **Disciplinary Procedure:** Same as above.  |
| Removal of records, passing [COMPANY NAME] classified Information **(such as customer cardholder data)** for personal gain, or possession and removal of reports, not required for business purposes, with the intention of utilizing for financial or personal gain.  | **Medium Risk** This is a breach of confidentiality agreements and deviates from security policies. **Disciplinary Procedure:** Same as above.  |
| Utilizing personal laptops, PCs, any such data processing/computing devices, without permission or knowledge of both and direct management. Where connected to [COMPANY NAME] LAN. | **Medium Risk** No machines should be connected to any [COMPANY NAME] Network unless fully loaded with [COMPANY NAME] approved software, including Microsoft Windows products and anti-virus software protection. All the software must be licensed to [COMPANY NAME]. (No illegal software is permitted). **Disciplinary Procedure:** Same as above  |

1. Workstations Usage User Agreement

[COMPANY NAME] contractors, temporary staff, and vendors must sign a Non-Disclosure Agreement (NDA).

1. Non-Conformance

All [COMPANY NAME] staff members, respective outsourced parties, must familiarize themselves with this policy and adhere to it at all times.

1. Security Incident Reporting

All breaches of security policies that pose a threat to or show weakness in [COMPANY NAME] environment must be reported immediately to the HEAD OF IT.

1. Information Security Violation Escalation

This procedure describes the steps to be taken when a Information Security Violation of any type or severity level is discovered at [COMPANY NAME].

Following this procedure would expedite the process to investigate potential Information Security Violations, and help to contain any possible damage or adverse effects to [COMPANY NAME] information and privacy.

These procedures cover all [COMPANY NAME] workstations and communications equipment’s, operating systems, applications, and networks, whether or not they are connected at [COMPANY NAME] sites or division. The procedure also covers non-[COMPANY NAME] workstations, communications equipment’s, operating systems, applications, and networks, which are either directly or indirectly linked to [COMPANY NAME] systems or are used for the development and/or maintenance of [COMPANY NAME] hardware or software.

1. Responsibilities

It is the responsibility of:

* All Users of [COMPANY NAME] workstations and communications equipments, operating systems, applications and networks to inform when a suspected Information Security Violation is discovered on any [COMPANY NAME] workstations, communications equipment, operating systems, applications and networks.
* HEAD OF IT to investigate every reported violation.
* HEAD OF IT to notify the Manager(s) of the user who caused the violation (i.e., violations of a disciplinary nature), of the investigation, including any details discovered to date, the potential severity of the violation, and the risks involved in that violation.
* HEAD OF IT to notify Human Resources and Internal Audit of the investigation, in order to obtain their assistance. (In cases where disciplinary action is called for).
* Internal Audit staff to provide their assistance and expertise in the investigation of the suspected violation.
* Human Resources Department staff to take appropriate action upon the results of the investigation, in concert with the Manager(s) of the suspected individual(s), the Internal Audit, and the HEAD OF IT.
* All the parties involved, to ensure the privacy of the individual(s) under investigation, both during and after the investigation.
1. Definitions

|  |  |
| --- | --- |
| **Category 1** | Minor Information Security Violation with no significant impact.  |
| **Category 2** | Medium Information Security Violation with low impact. |
| **Category 3** | Major Information Security Violation with medium impact. |
| **Category 4** | Critical Information Security Violation with serious impact. |
| **Evidence** | All materials collected which prove or disprove a suspected Information Security Violation. |
| **HRD** | Human Resources Department |
| **IA** | Internal Audit  |
| **HEAD OF IT** | Head of Information Technology Department |
| **Impact** | Level of damage caused by Information Security Violation. This level can be a combination of direct financial loss, indirect financial loss, and violation of applicable local laws, loss of system or network access, public embarrassment, potential civil or criminal lawsuits against [COMPANY NAME]. |
| **Information Security Violation** | Any action which is in opposition to current [COMPANY NAME] policies, procedures or standards regarding Information Security in whatever form. |
| **Suspect** | Person(s) who may have violated security policies, procedures or standards. Suspects will be treated, as innocent until proven guilty. |
| **Worm** | Self-replicating workstations program which can cause loss of programs, data or functionality. |

#

1. Information Security Violation Escalation Procedure

If a Information Security Violation of any magnitude is found or suspected, individual User should follow the steps indicated below:

| **Step** | **Done By** | **Step Detail** | **When** |
| --- | --- | --- | --- |
| **1.** | [COMPANY NAME] Staff (user) | [COMPANY NAME] Staff must contact the line manager with details of the potential violation. | When a possible Information Security Violation is discovered or suspected. |
| **2.** | HEAD OF IT | Complete a Information Security Violation Investigation Form (Annexure - 1) with the following details - Name of Person making the claim.Date and Time of NotificationDepartment or Area where violation occurred.Date and Time of suspected violation.Name(s), IP address (es) of Suspect(s), if known.Specific Violation or Problem encountered in detail.Security Impact (if known).Business Impact (if known). | Upon notification by [COMPANY NAME] Staff, or upon discovery within HEAD OF IT. |
| **3.** | HEAD OF IT | Make an initial classification of the suspected violation, based on the **1.14. Information Security Violation Category.**  | Initial notification occurs. |
| **4.** | HEAD OF IT | Contact Manager of Suspect(s), informing him/her of the investigation and the initial severity level, for Categories 2, 3 and 4.  | Upon determination of initial severity level. |
| **5.** | HEAD OF IT | Enter details from Information Security Violation Investigation Form into [COMPANY NAME] Information Security Violation Database.Check Information Security Violation Database for any previous investigations against Suspect(s). Check for any patterns.Check Information Security Violation Database for any previous claims by person(s) reporting the incident. Review any previous violations. Check for any patterns.Perform initial investigation to verify category of incident.Gather all evidences pertaining to the Suspect activity. Determine if further investigation is warranted. | Upon determination of initial severity level, and notification of Manager of Suspect(s) where applicable. |
| **6.** | HEAD OF IT | Check previous violation reports. If multiple Category 1 violations have occurred on the same problem or area, escalate to Category 2.If Information Security Violation is Category 1 only, and evidence confirms this, contact the Suspect directly and note the problem. State that the problem is not serious, but to be more careful in the future.  | When Category 1 has been confirmed. |
| **7.** | HEAD OF IT | If Information Security Violation is Category 2 only, and initial evidence confirms this, notify Manager of Suspect(s) of the situation.Arrange meeting between HEAD OF IT, Suspect(s) and Manager of Suspect(s).Review any previous violations (Category level 1) and determine if a pattern can be found.Note problem(s) encountered and provide Suspect(s) with a formal written notice of the violation. Inform Suspect(s) that this information will be placed in their Personnel file, and will be considered in future actions by the [COMPANY NAME].Formal written notice must be signed by HEAD OF IT, Suspect(s) and Manager of Suspect(s).Provide Suspect(s) with a copy of the formal written notice, forward a copy to Human Resources for inclusion in Suspect(s) personnel file. | When Category 2 has been confirmed. |
| **8.** | IT | If Information Security Violation is Category 3 only, and initial evidence confirms this, notify the following:- * Manager of Suspect(s)
* Head of Department
* Internal Audit
* Human Resources

Co-ordinate investigation between areas concerned.Ensure Suspect(s) are not informed of investigation at present.Place Suspect(s) workstations access under surveillance, activating audit trails and/or specific security reporting tools where applicable.Do not restrict Suspect(s) workstations access at present, unless clear evidence suggests possible escalation to Category 4 is imminent. Gather all the relevant evidence concerning the Information Security Violation. Ensure that evidence is documented and that any mitigating evidence is included.Review any previous violations (Category levels 1 and 2) and determine if a pattern can be found. | When Category 3 has been confirmed. |
| **9.** | Human Resources | Determine disciplinary actions to be taken, in conjunction with IT, Internal Audit and Manager of Suspect(s).The action to be taken against the individual/group violating the policy shall be in line with the Human Resource policy | Upon completion of Step 8. |
| **10.** | HEAD OF IT | If Information Security Violation is Category 4 only, and initial evidence confirms this, notify the following:- * Manager of Suspect(s)
* Head of Department
* General Manager
* Internal Audit
* Human Resources

Co-ordinate investigation between areas concerned.Ensure Suspect(s) are not informed of investigation at present.Place Suspect(s) workstations access under surveillance, activating audit trails and/or specific security reporting tools where applicable.Restrict Suspect(s) workstations access, if the evidences suggest a Category 4 Information Security Violation Incident.Gather all the relevant evidence concerning the Information Security Violation. Ensure that evidence is documented, and that any mitigating evidence is included.Review any previous violations (at any Category levels 1, 2 and 3) and determine if a pattern can be found. | When Category 4 has been confirmed. |
| **11.** | IT,Human Resources,Internal Audit,Physical Security Officer(s),Manager of Suspect(s), | Arrange meeting between HEAD OF IT, Human Resources, Internal Audit Department, Suspect(s) and Manager of Suspect(s).Note problem(s) encountered and provide Suspect(s) with a formal written notice of the violation, and that this violation calls for immediate termination of employment by [COMPANY NAME].Inform Suspect(s) that they are liable for any damages caused by their actions, and that said damages will be deducted from their final pay. Inform Suspect(s) that their actions are subject to criminal prosecution. Due to this, have Suspect(s) arrested during meeting.Suspect(s) must be escorted from meeting area by Security Guard(s) to their work area, along with Manager. Suspect(s) must remove all personal property, but may remove no workstations media of any type, whether they own the media or not. Security Guard(s) must obtain all [COMPANY NAME] property from the Suspect(s), including ID cards, smart cards, keys, etc. | Termination of employment is the only course of action in all Category 4 instances. |

#

1. Information Security Violation Category
* **Category 1**: Minor Information Security Violation with no significant impact

Examples - Attempted (and failed) read of a file, password revoked from invalid attempts, finding a virus.

* **Category 2:** Medium Information Security Violation with low impact

Examples - Repeated (and failed) attempts to read the same file over a period of time, failed attempt to log on with someone else's User ID and password, sending an e-Mail attachment with a virus (presumably by accident).

* **Category 3**: Major Information Security Violation with medium impact

Examples - Successful attempt to read an unauthorised file, use of someone else's User ID and password, knowingly collecting/developing/distributing a virus, possession of anti-security software (password crackers, hacking tools, network monitors, sniffer tools, etc.), possession of legal pornography.

* **Category 4**: Critical Information Security Violation with serious impact

Examples - Successful attempt to change or delete unauthorised file, use of anti-security software, key loggers, possession of illegal pornography, distribution of pornography, attempts (failed or successful) to transfer confidential data illegally, theft of equipment from [COMPANY NAME], theft of business information for sale, electronic blackmail of [COMPANY NAME].

1. Procedures for making Amendments to Policies

**15.1 Guidelines**

#### All Amendments to this policy should be done only by the IS Security manager. It should be ensured that frequent changes are not made to the document, unless they are strategic in nature.

#### All changes have to be recorded in the Change control form.

#### The Change control form should be reviewed by the General Manager and subsequently by the Board of Directors.

1. Annexure 1: Information Security Violation Investigation Form

**Information Security Violation Investigation Form**

Reference Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1. Reporter Information:**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Emp. No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Tel. Extn.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Section: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User/Logon ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date reported: \_\_\_\_\_\_\_\_\_\_\_ Time reported: \_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2. Suspect’s Information:**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Emp. No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Tel. Extn.:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Section: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User/Logon ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ IP Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date of incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Time of incident: \_\_\_\_\_\_\_\_\_\_\_\_

**3. Details of Suspected Information Security Violation:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4. Initial Violation Category:**

🞏 Category 1 🞏 Category 2 🞏 Category 3 🞏 Category 4

**5. Details of Investigation:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6. HEAD OF IT:**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_