PISM-904 Security Incident and weakness Management Procedure

Revision / Version	**Date**	**Comments**
1.0	25/01/2010	Nil
2.0	28/06/2013	Nil
3.0	04/02/2016	Addition of escalation matrix
3.1	07/04/2017	Change in communication Matrix and addition in incident handling
3.2	24/04/2018	Change in communication Matrix

Security Incident and Weakness Management Procedure

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to describe the processes to be followed by users to report suspected or actual Information Security Incidents. The aim is to standardize the reporting process for users in respect of suspected or actual Information Security incidents. It is acknowledged by the organization that discipline is a necessary way of ensuring that Information Security incidents are dealt with in a fair and effective way wherever extreme carelessness or apparent misconduct is involved.

Target audience of this process is ISM, Senior Management and all associates of SYBRID.

1.2 Responsibilities

Information Security Manager is the owner of this process and is responsible to ensure compliance.

It is the responsibility of ISM to communicate to the associates that it is important to report suspected incidents and weaknesses, even if they later prove to be simple errors.

2 Procedural Description

2.1 Incident Reporting

The Incident Management Process initiates when a user submits the RISM 902 - Information Security Incident and Weakness Reporting Form to respective department head for investigation and keeping ISM in loop (CC), or communicates the critical incident or weakness to respective department head via Phone call when immediate action is required to overcome the situation.

Two main categories of the incident reporting are:

- Reporting Information Security Breach
- Reporting Information Security Weakness

On first noticing the Information Security Breach / Weakness witness notifies the immediate line manager, respective department and the ISM immediately. Witness will fill out the form and send it to concern department and keep ISM in loop as soon as possible after a suspected security incident or weakness is observed.

Form is available online **(Click Here)**. Alternatively, printed version can also be filled out and send to concern department head.

Information security incident/weakness should be reported through following communication matrix. Internal and external parties i.e. (visitors, clients, contractors and vendors) can also report any information security incident or weakness through "Incident Reporting Drop Box".

Note: External parties i.e. visitors, clients, contractors and vendors are not required to follow formal process they can just report security weakness incident by dropping the form in drop box.

Communication Matrix for Information Security Incident and Weakness Reporting

Type of Indent/ Weakness "Example"	Department to be Involved	Person to be Involved	E-mail Address	Extension #	Cell #
Physical Security Breach/ Weakness	Administration	Mr. Fazal Imam (Khi)	fazal.imam@sybrid.com	5641	0300-2006345
		Mr. Humayun Iqbal (Isb)	humayun.iqbal@sybridts.com	6001	0347 9371000
IT related weakness/Incidents/ Virus/ Malicious Attacks/ Software malfunctions	Information Technology	Mr. Saad Ullah Khan	Muhammad.saad@sybrid.com	5996	0301-8223508
Any Security Weakness/Incidents related to in house developed CRM/Module/Workflows etc.	Solution Development Group	Mr. Naseer Ahmed	naseer.ahmed@sybrid.com	5742	0301-8254414
Security Weakness related to Human Resource/ Misconduct/ Violation HR Policies.	Human Resource Department	Mr. Atif Sattar	atif.sattar@sybridts.com	5962	0347-9371006
Noncompliance with policies/ procedures and guidelines	Quality Assurance	QA Team	qa@sybrid.com	5665	0345-3176805

Note:

- ISM will be in loop in every incident and weakness reporting correspondence
  ISM e-mail: salman.ahmed@sybrid.com

- If there is any ambiguity while reporting the incidents and weaknesses the employee may discuss with ISM for clarity.
- If the incident reporting is done via phone, then the employee must also submit the incident formally within 24 hours.

2.2 Incident Handling

The head of concern department upon receiving the incident reporting form ensures the completeness of the form and classifies the incident based on the incident type. Incidents could be of following types:-

- System malfunction or overloads
- Human errors
- Non-compliance with policies or guidelines
- Breaches of physical security arrangements
- Uncontrolled system changes
- Malfunction of software or hardware
- Access violations
- Loss of service, equipment or facilities
- Uncontrolled/unlabeled documents seen
- Business Impact/Cost: Incidents will also be classified based on their business impact. They can be classified as:
  - **Critical:** System/device down; is causing work to cease. SYBRID is in danger of or is experiencing a financial loss, or the ability to make strategic business decisions is impaired. No work around available.
    - Affects Large Number of Users
    - Production Server Down
    - Router Down
    - Office Can't Send Mail
    - Office Can't Receive Mail

- Physical Intrusion
  - **High:** Level of service degraded or system/device down causing work to cease and potential business impact. Work around may not be available.
  - **Medium:** Work continues (e.g. unrelated to the failing component or as a result of implementing a work around) though operational impact is being encountered (e.g. data is occasionally lost). Work around exists if needed.
  - **Low:** Work continues (e.g. unrelated to the failing component or as a result of implementing a work around) though personal impact is being encountered (e.g. consumer time is occasionally lost, consumer is frustrated) work around exists if needed.

Incident Frequency: Incident will also be classified by their frequency of occurrence. Incident can be one of the following levels:

- ~~Rush:~~Very Often: Incidents which occur on regular basis. More than 15 instances per quarter
- ~~High~~Often: Incidents which occur on less regular basis but has more than 10 instances per quarter
- ~~Medium~~Sometimes: Incident's which occur on occasional basis. More than 5 instances per quarter
- ~~Low~~Rarely: Incident's which occurrence is very low. Occurred once a quarter

Formatted: Not Highlight

This classification of incidents helps to provide the corrective action accordingly.

Concern department's head then isolates the affected area if possible and collects the evidence. It is also very important to keep the record of the evidence securely whether it's a paper document , any physical equipment or information on hard disks, storage media etc. Moreover, it should be considered that in case of paper document where was it found, when was it found and who witnessed the discovery.

Concern department's head ~~–~~then calls a suitable incident response team which is capable of responding to the reported incident. The makeup of this team may include:

- HR Representative - to help deal with potential disciplinary actions
- Technical Representative - to help understand the nature of the incident
- Line Management Representative
- Facility Administrator - to clarify any physical access issues

Depending upon the severity of the incident additional resources may be required:

- Law Enforcement Agency Representative
- Third party specialist(s)

Note: Incident response team may speak with media and law enforcement agencies if it is required.

~~Depending upon the severity of the incident additional resources may be required:~~

- ~~ISMF~~
- ~~Law Enforcement Agency Representative~~
- ~~Third party specialist(s)~~

Once the team is assembled, an initial meeting is held within 48 hours to consider the following:

- Current status of the incident
- Escalations as required
- Detailed description of the incident, including any technical information
- Potential Impact of the incident
- Suggested initial response plan

Actions required closing the incident. It is important to learn from the incidents to avoid future problems or if they occur again so they can be dealt more effectively. It also helps to identify where the controls do not work as intended, and where improvements are necessary.

All these actions along with the details of the incidents are recorded into **"Root Cause Analysis Log Sheet"** RISM 906 - Root Cause Analysis Log Sheet

This log sheet will be reviewed by the ISM and ISMF on Bi-Annual basis. This report will also be discussed during management reviews.

2.3 Incident Review

The records of the incidents reported are maintained and reviewed. ISMF reviews the list of all the reported incidents at ISMF Review Meetings. Points to review include:

- Status of the Incident
- No. of Incidents Reported
- Adequacy of actions taken to resolve the incident
- Preventive Measures

In case it is found out that a particular incident raised in past is still not resolved suitably, incident handling process will be triggered again. For all the incidents closed appropriately, report will be generated and incident will be closed but still kept in record.

For recurring incidents reasons will be found out and appropriate controls will be suggested to cope up with the problem.

This is the responsibility of respective department head to provide immediate response containing corrective actions taken to persons reporting information security incident and weakness after the issue dealt with and closed.

3 Guidelines of Incident Handling

In addition to normal contingency plans the guidelines are established to cover the analysis and identification of the cause of the incident, containment, planning and implementation of corrective actions to prevent recurrence, communication with those affected by or involved with recovery from the incident and reporting the action to the appropriate authority

There are following procedures in place to deal with incidents as per their classification.

1. Handling of Physical Security Incidents
2. Handling of Hardware Incidents
3. Handling of Software and Business Data Incidents
4. Handling of Services Failure Incidents

The reported incident will be handled keeping in view the category in which the incident falls. This categorization is done by concern departmental head and ISM after initial analysis of the incident. Handling of each category is described as separate procedure and is mentioned in detail below:

3.1 Handling of Physical Security Incidents

If the reported incident falls in the category of violation of physical security, then the severity of the incident will be determined.

If the incident is of critical nature it might invoke the disciplinary action process. Investigations can be carried out by looking at the CCTV recordings, by asking other associates and taking interview of the person who reported the incident. All the findings of the investigation must be kept confidential and the details must be logged in the incident record sheet.

Few of the physical security violations can be unauthorized access to a secure area or premises, theft of company assets, breaches of physical security arrangements, loss of equipment or facilities, power failure, fire or any other natural disaster or misuse and damage of information processing systems.

3.2 Handling of Hardware Incidents

When the hardware failure is reported by an associate, head of department will carry out the initial investigations to find out the owner of the hardware and then the reason for failure and the severity of problem.

In case the problem can't be handled internally the vendor of the hardware will be called to resolve the issue. If the device is to be taken out of the premises then necessary action will be taken such as data omission and protection, backup will be arranged.

If a hardware malfunctions because of mishandling, then the information security incident will be raised and it might lead to user awareness training in order to avoid its recurrence in future, but due care should be taken of the confidentiality aspects.

3.3 Handling of Software and Business Data Incidents

Software incidents are further classified into following categories:

- Application failure
- OS failure
- Server failure
- Virus
- Uncontrolled system changes
- System malfunctions and overload

In case of information system failure or malfunctions, incident must be raised immediately and it will be referred by ISM to the appropriate personnel for investigation and analysis. If software gets corrupt, IT is responsible to provide assistance in this case.

If the data is misused by an associate, disciplinary action will be called to investigate further and reasons will be found out for the misuse.

3.4 Handling of Services Failure Incidents

In case of service failure, backup will be provided to ensure smooth business continuity.