SECOVA™

Incident Management procedure

Marketing Copy

Scope

This procedure covers the complete incident management activities of the organization. This process applies to all Secova businesses on a twenty-four hours a day, seven days a week (24X7) basis, and applies to all Secova-related internal and external Information Security incidents

1. Responsibility

- CISO is the owner of this procedure
- All employees/contract staff are responsible for timely notification of security incidents
- The **ISF team** would oversee the handling of the security incidents.
- Top Management is responsible for the authorizing action items, approve changes to the procedure

2. Activity

An information security incident is defined as:

- An actual or possible security breach to one or more Secova information assets.
- Any adverse event which occurs either internally or at an outside vendor whereby the confidentiality, integrity or availability of Secova Information could be threatened. This may involve accidental or intentional damage, disclosure, loss, misuse or theft of Secova's information or technology assets.
- The unauthorized use of Secova technology resources for purposes other than conducting company business.
- Examples of Security Incidents
    - Inadvertent or intentional disclosure of customer data, including Restricted or Confidential data
    - Loss or stolen laptops, hard disks, or data storage devices
    - Improper handling or disposal of data
    - Denial of service attacks
    - Unauthorized changes to configurations, code or data
    - Unauthorized sharing of Secova system configurations, code, data or information in chat rooms on the Internet or publicly
    - Significant violation of Secova Information security Policies and Standards
    - Sharing or unauthorized use of passwords
    - Unauthorized access to systems or information

Incident Reporting

- Information security weaknesses and events are reported, immediately they are seen or experienced to the ISF team through either email or Phone.

- Users are not allowed to continue working after identifying a possible weakness or information security event
- If a potential breach involves restricted or confidential data, the incident would be deemed a Security Incident and this process would be invoked. Some scenarios are more obvious than others. If there is any possibility that Restricted or Confidential data was inadvertently disclosed, please contact Information Security team member immediately. The ISF team records the incident. **(Refer Template: A.13.1 Security Incident Management Report)**

Incident Responding

- All information security events and weaknesses are, immediately upon receipt assessed and categorized by the ISF team. Initially, there are four categories: events, weaknesses, incidents and unknowns.

  "Events" are occurrences that, after analysis, have no [or very minor] importance for information security;

  "vulnerabilities" are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security;

  "incidents" are occurrences of events (series of events) that have a [significant] probability of compromising the Organization's information security;

  "unknowns" are those reported events or weaknesses that, after initial analysis, are still not capable of allocation to one of the four categories.
- The "unknowns" are subject to further analysis to allocate them to one of the other three categories as soon as possible.
- The prioritization for responses, when there are multiple event reports to deal with, is: incidents, unknowns, vulnerabilities, events.
- When there are multiple event reports in each category, the Information Security Manager prioritizes responses in the light of the criticality of the business systems and information assets at risk, the danger of further compromise to the Organization's information security, and the resources at his disposal.
- Specific Work Instructions set out the necessary containment and corrective action and standing contingency plans in respect of the following types of information security incident:
  - Systems failure and loss of service
  - Malware, including viruses
  - Denial of service
  - Errors resulting from poor data
  - Breaches of confidentiality
  - Breaches of information integrity
  - Misuse of information systems
  - Non-standard incidents

- The IT manager seeks additional input from qualified technical staff, as necessary and where he considers the standing instructions to be inadequate, to analyze and understand the incident and to identify appropriate actions to contain it and to implement contingency plans.
- The Information Security Manager invokes actions as set out in the standing Work Instructions plus additional activity that he considers necessary to contain and recover from the incident, and to implement contingency plans.
- The Information Security Manager confirms that the affected business systems have been restored and that the required controls are operational before authorizing a return to normal working.

Learning from the Incident

Once the incident is contained, and the required corrective action is completed, the ISF team reports to the CISO with

- a summary of the incident,
- identifying the cause of the incident and analyzing its progress,
- trying to identify how the Organization could have responded earlier or more effectively,
- preventive action that might have been taken in advance of the information,
- the effectiveness of the containment and corrective actions and the contingency plans, and
- how the incident was closed out

Evidence collection and Analysis

The Information Security Manager is responsible for closing out the incident:

- this includes any reports to external authorities;
- initiating disciplinary action by referring the incident to the [Head of HR];
- planning and implementing preventative action to avoid any further recurrence;
- collecting and securing audit trails and forensic evidence;
- Initiating any action for compensation from software, service suppliers by referring the incident to the Head of Admin, and communicating with those affected by or involved in the incident about returning to normal working and any other issues.
- The ISF team prepares a monthly report to the which identifies the number, type, category and severity of information security incidents during the preceding month, the cost of containment and recovery, and the total cost of the losses arising from each incident, and recommends (where appropriate) additional controls that might limit the frequency of information security incidents, improve the Organization's ability to respond, and reduce the cost of response.
- All the incident reports from the period since the last management review are taken into account at the next one, to ensure that the Organization learns from the incidents.

Security Incident Handling

STEP 1: Identify the Nature of the Security Breach

Type: Physical Security Breach – includes break-in, glass breakage, stolen equipment, etc.

Type: Data Breach – includes Customer data, breach of IT systems that may involve Customer data, documents containing information on Customer employees

STEP 2: Make Emergency Notifications

Immediately contact the following individuals:

The ISF team would notify the CISO for all emergency notifications. The CISO would decide if the incident needs to escalated further and may communicate to the senior management accordingly for approval/actions

The ISF team would work with location specific list of contact personnel for incident handling

STEP 3: Secure the Area Breached

Type: Physical Security Breach – ensure at least one person remains in the area of the intrusion until local authorities arrive and the facility can be secured. The site Operations Manager will contact a locksmith or glass company to repair any damaged entryways and secure the building. Restrict access to the site to only Secova managers or authorities.

Type: Data Breach – lockdown all equipment that is being used to manage Customer data or documents. Restrict access to equipment until extent of breach can be determined by IT personnel.

STEP 4: Protect evidence and Chain of Custody

Do not move anything or allow anyone else to move company materials or potential evidence until authorities or the Operations Manager has approved it. Any materials or equipment retained by Secova after a security breach must be secured until processed and the extent of the breach determined. Data / document breaches, especially, require Secova personnel to control access and chain of custody until released by Secova senior management.

STEP 5: Communication of Security Incidents to external parties

(External Parties refer be customers, legal authorities, regulatory bodies). This can be initiated only by the following personnel

Executive Team of Secova

SLAs for Incident Handling

Following are the current SLAs defined for Incident Management

Severity Level/ Impact Assessment	Description	Timeframe to Notify Client
5 – Low*	Incident where the impact is minimal. Examples are isolated malicious virus infections, accidental violation of process or procedure, and minimal unsuccessful *non-intelligent* attempts to breach a Low or Medium Criticality system.	72 hrs
4- Medium*	Incident where there may be moderate impact to a Business. Examples include *intelligent* unsuccessful attempts to breach any Criticality system, multiple unsuccessful *non-intelligent* attempts to breach any Criticality system, multiple reports of malicious SPAM or virus within a Business, theft of Client Internal Information, unexplained system failures or outages, possible or actual minor suspicious business interruption.	Within 24 hours after incident detection
3- High	Incident where the impact to a Business may be serious. Examples include malicious intent, internal wrongdoing, *possible* breach of any Criticality system, *actual* breach of Low or Medium Criticality system, compromise of Client information classified as Confidential, hacker websites that harvest customer information, moderate business interruption, simultaneous system outages, breach of Local Laws.	ASAP but not to exceed 4 hours after incident detection
2- Very High	Incidents where the impact to a Business may be severe and represent a crisis to the Business, or where the impact to the Franchise may be serious. Examples include possible or actual serious Business disruption, possible breach of multiple systems of any Criticality, compromise of Client Highly Confidential Information, *actual* breach of High Criticality level system.	ASAP but not to exceed 2 hours after incident detection
1- Critical	Incidents where the impact to the Franchise may be severe and represent a crisis to the Franchise. Examples include possible disruption of multiple businesses, compromise of Client Information classified as Restricted, or significant public impact to Client's reputation or regulatory posture.	ASAP but not to exceed 1 hour after incident detection

3. Records

1. Incident reports
2. Evidences of security violations