Incident Management Policy v4.4

Master List Ref	Release Date	Review Date	Next Review Date
PL-ISMS-ENT-004	January, 2016	January, 2024	January, 2025
Version:	**Process Owner**	**Reviewed by**	**Approved by**
4.4	IRM	Shamba Gupta	Sameer Babu

Index

1. Reference

Information Systems (also referred to as the IS) are important business assets. Firstsource is committed to protecting its IS from acts of individuals or groups, either deliberate or accidental, which may compromise their Confidentiality, Availability or Integrity.

Firstsource is also committed to providing quality IT Services to its customers in line with ITSM specifications and contractual obligations.

2. Purpose

The purpose for publishing an Incidents Policy is to ensure that all security breaches and IT Services Incidents are reported, bringing to light all vulnerabilities in systems, processes or controls, to subsequently implement countermeasures or corrective actions and to build a knowledge base to minimize efforts for recurrences at other centres.

3. Scope

Firstsource shall formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its incident management program.

Any event that adversely affects or has the potential to adversely affect the Confidentiality, Availability or Integrity of Firstsource's IS and Quality of IT Services, is to be considered an Incident.

This policy applies to all personnel, systems, processes and controls at Firstsource.

- Security incidents would include incidents like Theft, virus attack, violation of Acceptable Use Policy etc., (security incidents list available at http://security.Firstsource.com) need to be reported.
- Privacy breach incidents shall be reported as per the Data Privacy Policy (PL-ISMS-ENT-012);
- IT Services Incidents would include incidents like, Mail access problem, desktop hanging, network unreachable etc., (IT Services incidents list available with Central Support Desk, CSD and User Departments) need to be reported separately to IT team. These are not to be termed as Security Incidents.

4. Policy

4.1 Security Incidents Reporting

All incidents shall be reported to Central Support Desk (CSD) over the phone or using self-service tool (http://itsm.Firstsource.com/selfservice) by choosing "Security Incident" from the incident type drop down.

Firstsource shall follow Security Incidents Reporting process mentioned in PR-ISMS-ENT-014(Incident Management Procedure) ensuring that:

Security Incidents reporting shall happen immediately. Under no circumstances shall an employee delay reporting an incident.

- Irrespective of the time of the day (or night), all known details of the incident shall be provided over phone (one shall not for example, send an email and consider having fulfilled one's responsibility).
- Once the Incident is reported, the CSD shall take the security incident details as per the format available with them and in turn inform the Security Team to initiate investigation immediately.
- Incidents that relate to client (processes and data confidentiality), shall also be reported by the CSD to the client Operations/Relations Manager, who in consultation with the IRM team shall keep the client updated on the Incident and its investigation developments.

- Organization-wide standards shall be specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that will be included in the incident notification.
- Firstsource IRM Team / Procurement Team / Legal Team will further maintain a list of third-party contact information which can be used to report a security incident. Reporting of any security incident/risks will be according to the guidelines stated in Cyber Security Manual.
- Firstsource shall implement an insider threat program that includes a cross-discipline insider threat incident handling team.
- Firstsource shall provide a process/mechanism to anonymously report security issues.
- The incident management program shall formally define information security incidents and the phases of incident response; roles and responsibilities; incident handling, reporting and communication processes; third-party relationships and the handling of third-party breaches; and the supporting forensics program.
- Firstsource shall formally assign job titles and duties for handling computer and network security incidents to specific individuals and shall identify management personnel who will support the incident handling process by acting in key decision-making roles.
- Reports and communications shall be made without unreasonable delay and no later than 60 days after the discovery of an incident, unless otherwise stated by law enforcement orally or in writing and include the necessary elements.

Strict confidentiality is of utmost importance while reporting an Incident. All Incidents automatically fall under the category of Firstsource Confidential (as described by Firstsource Information Classification guidelines) with the Head-IRM/Risk Committee as the owners of the Information.

- The employee and the Line Manager shall not discuss the Incident with anyone else other than the IRM Team or the RISK COMMITTEE member till such time that the RISK COMMITTEE or IRM Team formally communicates that the Incident has been declared Firstsource Public.
- The IRM Team and the RISK COMMITTEE member may disclose partial or full details of the Incident to other employees or contractors if required for the purpose of investigating the Incident or for information purposes.
- Once the Incident investigation has been completed, the Incident details and the countermeasures of level 1, 2 & 3 incidents shall be presented to the RISK COMMITTEE by the IRM Team. Details of the RISK COMMITTEE can be found in the Firstsource IS Cyber Security Policy(ISMS-001) under the Security Organization section.
- Security incidents may be anonymously reported at CSD over the phone.
- Any press release regarding Incidents shall have the CEO's written clearance.
- The Head-IRM/RISK COMMITTEE may also divulge details of Incidents to law enforcement or regulatory bodies where required.

4.2 IT Services Incidents Reporting

IT Services Incidents shall also be reported at CSD over the phone or by using self service tool by all the user departments. Procedures shall be adopted to manage the impact of service incidents.

Procedures shall define the recording, prioritisation, business impact, classification, updating, escalation, resolution and formal closure of all service incidents.

The users shall be kept informed of the progress of their reported incident and alerted in advance if their service levels cannot be met and an action agreed. Major incidents (Service Outages) shall be classified and managed as per Problem Management Process and Procedure.

5. Incident Handling

All IT incidents & service shall be handled as per the Incident Management Procedure PR-ITSM-ENT-110 (external document).

All security incidents shall be handled as per the Incident Management Procedure PR-ISMS-ENT-014.

5.1 Disciplinary Process

Firstsource shall follow disciplinary process mentioned in PR-ISMS-ENT-014 (Incident Management Procedure) ensuring that:

- Sanctions are fairly applied to employees following violations of the information security policies once a breach is verified and includes consideration of multiple factors and maintain the record of person involved and the outcome.
- A list of employees involved in security incidents is maintained with the resulting outcome from the investigation.
- A contact in HR is appointed to handle employee security incidents and notify the Head-IRM or a designated representative of the application of a formal employee sanctions process, identifying the individual and the reason for the sanction.

5.2 Prevention of Misuse of Information

Firstsource shall prevent the misuse of assets following the process mentioned in PR-ISMS-ENT-014 (Incident Management Procedure) ensuring that:

- Management approval for the use of information assets is taken and Firstsource shall take appropriate action when unauthorized activity occurs.

5.3 Incident Response Testing

Firstsource shall follow Responsibilities and Procedures mentioned in PR-ISMS-ENT-014 (Incident Management Procedure) ensuring that:

- Firstsource shall test and/or exercise its incident response capability regularly.
- Testing exercises shall be planned, coordinated, executed, and documented periodically, at least annually, using reviews, analyses, and simulations to determine incident response effectiveness.
- Testing shall include personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

5.4 Learning from Incidents

Firstsource shall follow process of Learning from Incidents mentioned in PR-ISMS-ENT-014 (Incident Management Procedure) ensuring that:

- The information gained from the evaluation of information security incidents shall be used to identify recurring or high impact incidents and update the incident response and recovery strategy.
- Firstsource shall implement an incident handling capability for security incidents that addresses references to a vulnerability management program to manage the incidents.
- Firstsource shall coordinate incident handling activities with contingency planning activities.

Annexure A

Information Classification Details

Classification: Firstsource Restricted
Information Owner (IO): RISK COMMITTEE
Information Custodian (IC): IRM Team
Authorization List (AL): RISK COMMITTEE; Software, HR, Admin and Technology Teams
Declassify on: Never

Annexure B

Changes since last versions

Date	Version Number	Changes made
5th May, 2006	v3.1 to v4.0	1. Nomenclature changed. 2. Document references changed.
5th Jan, 2011	v4.0 to v4.1	1. Updated section 5 to link with appropriate procedure documents.
2nd Jan, 2012	v4.1 to v4.2	1. Updated scope to include Privacy breach incident reporting
January 4, 2016	v4.2 to v4.3	1. Replaced InfoSec team with IRM team.
January 3, 2017	v4.3	1. No updates
22nd Dec, 2020	v4.3 to v4.4	1. Updated few incident management procedures