Cyber Security

Policy v16.2

Master List Ref	Release Date	Review Date	Next Review Date
ISMS-001	December, 2019	January, 2025	January, 2026
Version:	**Process Owner**	**Reviewed by**	**Approved by**
16.2	IRM	Associate Director - IRM	SVP - IRM

Index

1. Introduction

Firstsource Solutions Limited (henceforth referred to as Firstsource), is a leading provider of customised Business Process Management (BPM) services having its offices in India, Philippines, United Kingdom, United States, Mexico, Australia and South Africa. It has multiple delivery centers and offers services to Banking & Financial Services, Healthcare, Telecom & Media, Insurance, Mortgages, Ed Tech and Utilities sectors.

Firstsource has adopted the ISO/IEC 27001 standard as its security framework; the **ISMS** (Information Security Management System) shall be established and maintained accordingly.

The ISMS shall apply to all its delivery centers (refer to Annexure E).

2.Security Commitment and Intent

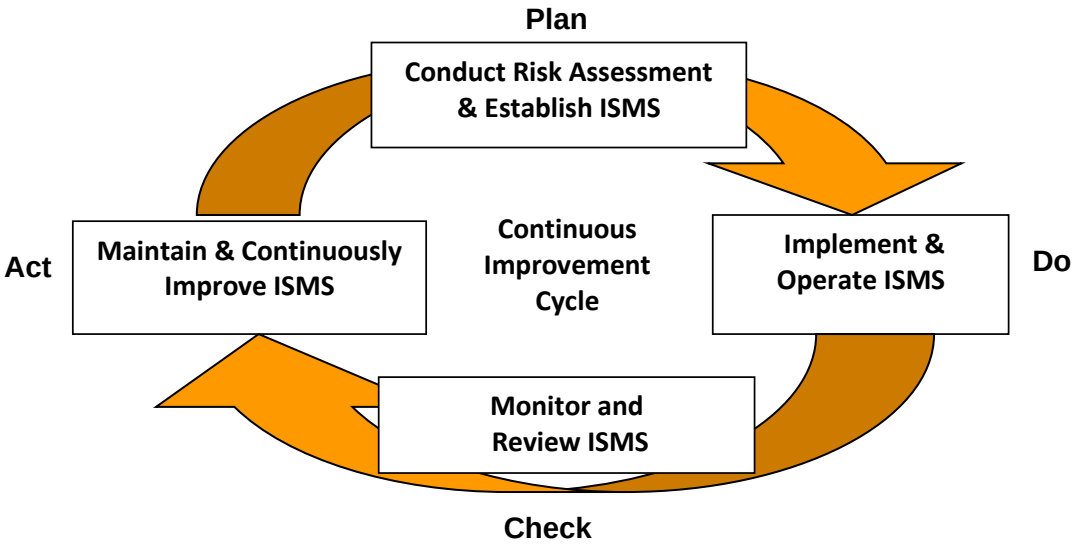
Firstsource is committed to provide a secure operating environment (maintain the **CIA** – **C**onfidentiality, **I**ntegrity and **A**vailability of all Information and Information Systems) to all its clients. An **Information Security Policy Statement** (Annexure D) signed by the Managing Director and CEO, to this effect, shall be published and displayed prominently at all ISMS locations as well as be available to all on the information security intranet portal (http://security.firstsource.com).

3.Approach to ISMS

Firstsource ensures a continuous monitoring strategy and implements a continuous monitoring program that includes defined metrics to be monitored at least annually. Firstsource shall:

(i) establish defined metrics to be monitored annually at a minimum;
(ii) establish ongoing program assessments in accordance with its continuous monitoring strategy that includes, at a minimum: (a) annual compliance assessments across the entire organization, and (b) third-party independent compliance assessments performed annually.
(iii) ongoing status monitoring IAW its continuous monitoring strategy;
(iv) correlation and analysis of security-related information generated by assessments and monitoring;
(v) response actions to address results of these analyses; and,
(vi) reporting the cyber security state of the information system to appropriate organizational officials monthly and, if required, to external agencies as required by that agency.

A process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the ISMS shall be adopted.
In order to achieve the aforesaid, the PDCA (plan-do-check-act) model shall be applied to structure all ISMS processes.



The ISMS shall include the following:

- A Cyber Security Policies manual (this document, namely **ISMS-001**) to establish the primary policies; supporting policies, procedures and formats, shall be developed together to form the ISMS document tree;
- An enterprise wide RA (Risk Assessment) of all IT and Support services (F-ISMS-ENT-029) shall be performed annually;
- Firstsource shall report the security state of the information system to appropriate organizational officials monthly (if Encountered Example HIPPA Violation) and, if required, to external agencies as required by that agency.
- A **SoA** (Statement of Applicability) based on ISO/IEC 27001:2022 controls shall be prepared. Controls to be excluded or that are not applicable, shall be documented and properly justified in the SoA (PR-ISMS-ENT-002); as per the Risk Management Policy (PL-ISMS-ENT-008)
- The ISMS activities shall be monitored by the RISK COMMITTEE independently (for details, refer to section A.6.1.1); The ISMS activities will be reported to RISK COMMITTEE. Records of reporting shall be maintained for tracking and auditing purposes;
- A **security calendar** (GI-ISMS-ENT-003) shall be defined for plans related to security testing and to monitor the ISMS throughout the year; the calendar shall include but not be limited to technical compliance, physical security checks, training plan and operations process audits; and further Firstsource shall ensure that these activities are executed in a timely manner.
- The **RISK COMMITTEE directives**; The RISK COMMITTEE shall be the strategic advisor to the ISMS, approval authority for implementation of the ISMS and also approval authority for any residual risk controls plan ;
- Arrange for **external audits** through accredited certification bodies to verify ISO/IEC 27001:2022 compliance as per certification body norms.

4.Context of the organization

- The external and internal issues that are relevant to the organization and that affects its ability to achieve the intended outcome(s) of its ISMS shall be determined as per Annexure I;

- ISMS shall be developed, implemented, maintained and monitored and reviewed for continuous improvement as per the PDCA methodology (section 3, ISMS-001).

4.1. Organization and its context

There are no burning external or internal issues attracting immediate attention; however, the external or internal issues which are already identified or faced early, are been addressed via risk assessment.

4.2. Needs and expectations of interested parties

Firstsource shall determine:

a) interested parties that are relevant to the information security management system, as per Annexure J;
b) the requirements of these interested parties relevant to information security shall be as per Annexure J;

4.3. Scope of the information security management system

The ISMS boundaries shall be as follows:

- Business Activity: All processes required for Client Services Delivery, Project Transition, HR, Training, Physical Security, Facility, Administration, Quality, Legal and IT Support;
- Business Locations: As per Annexure E;
- IT Infrastructure: Information and Information Processing Assets used by the above mentioned business activities, located at the above-mentioned locations and to include all software development, support and maintenance activities.

4.4. Information security management system

4.4.1. Establish the ISMS

a) ISMS Policy

The Information Security Policies Manual (this document) contains the following:

1. Framework for the ISMS objectives and an overall sense of direction and principles for action with regards to Information Security;
2. Take into account business and legal or regulatory requirements, and contractual security obligations;
3. Establish the strategic organizational and risk management context in which the establishment and maintenance of the ISMS shall take place;
4. Establishes criteria against which risks shall be evaluated and the structure of the risk management shall be defined;
5. Shall be approved by the RISK COMMITTEE (any member in the RISK COMMITTEE group could approve), which represents the Management of the Organization.

b) Risk Assessment Approach

RA (Risk assessment) shall be performed at least once a year as per the Risk Management Policy (PL-ISMS-ENT-008) and shall take into account the business information security, legal and regulatory requirements. The Policy shall mandate that appropriate control objectives and controls be devised to reduce risks to acceptable levels. Risk acceptance criteria and the levels of risks that will be accepted shall be defined here. The Risk Assessment (F-ISMS-ENT-029) shall be signed off by the RISK COMMITTEE ensuring complete awareness of the residual

risks. Usage of the RA templates (F-ISMS-ENT-029) shall ensure comparable and reproducible results.

c) Risks Identification

1. An IT and Support services catalogue (F-ISMS-ENT-026) shall be established and documented;
2. Threats to the Information Assets shall be identified (F-ISMS-ENT-029);
3. The Vulnerabilities that could possibly exploit the threats shall be documented (F-ISMS-ENT-029);
4. The Impacts that losses of CIA are likely to cause shall be documented (F-ISMS-ENT-029).

d) Risk Assessment

1. Loss of business that might result from a security failure shall be assessed taking into account the potential consequences of a loss of CIA of the services and data assets;
2. Realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities and the controls that have been implemented shall be assessed;
3. The level of risk shall be estimated;
4. Based on criteria described in section 6.1.2 the level and types of Acceptable (residual) risks shall be described (F-ISMS-ENT-029).
5. The privacy, security and risk management program(s)shall be updated to reflect changes in risks.

e) **Risk Treatment** options shall be evaluated and selected from amongst the follows:

1. Appropriate automated controls shall be incorporated in the information system, supplemented by manual controls as needed;
2. The residual risks shall be identified and accepted as per the criteria established in the Risk Management Policy (PL-ISMS-ENT-008);
3. The Risk shall be avoided if possible, as per PL-ISMS-ENT-008;
4. The Risk shall be transferred to other parties (e.g. Insurance, supplier) as per PL-ISMS-ENT-008.

f) **Control Objectives and Controls** shall be identified and documented (ISMS-001) based on the Risk Management Policy (PL-ISMS-ENT-008) and the RA (F-ISMS-ENT-029). Control selection shall take legal, regulatory and contractual obligations into account.

g) **Control** objectives and controls shall be listed as Annexure A.

h) **Residual risks** (identified in F-ISMS-ENT-029) shall be duly approved by the RISK COMMITTEE;

i) **Management** approval for implementing and operating the ISMS shall be obtained and documented;

j) **SoA** (PR-ISMS-ENT-002) shall be prepared to include the following:

1. Control objectives and controls selected in 4.4.1.f and the reasons for their selection;
2. Control objectives and controls currently implemented as per 4.4.1.d.2;
3. Exclusion of control objectives and controls listed in Annexure A and their justifications

4.4.2. Implementing and Operating the ISMS

a) A Risk Treatment Plan detailing the controls shall form the comments field of the RA (F-ISMS-ENT-029)
b) The Risk Treatment Plan shall be implemented and their progress be tracked
c) Controls selected as per section 4.4.1.f shall be implemented and appropriate Records shall be generated and a list of the records shall be maintained (F-ISMS-ENT-006);
d) Effectiveness of the selected controls shall be measured as per the criteria described against each control in Annexure A; action to be initiated upon the measurement values shall also be defined in Annexure A;
e) Training and awareness programs shall be implemented as per section A.6.3;
f) Operations shall be managed as per various procedures listed in the Master List (F-ISMS-ENT-001);
g) ISMS resources shall be managed as per section 7.1;
h) Appropriate procedures and controls (GI-ISMS-ENT-002) shall be implemented to enable prompt detection and response to security Incidents.

4.4.3. ISMS Monitoring and Review

a) ISMS monitoring procedures shall be implemented for:
   - Detection of errors;
   - Identification of failed and successful security breaches and incidents;
   - Providing of management interfaces to ensure ISMS functioning as expected (Change control, Incident Management and Access authorization reporting, availability report of hosts, links and services, RISK COMMITTEE presentations);
   - Detecting incidents and thereby preventing them (reporting on IMS);
   - Determine effectiveness of incidence response by reporting and monitoring for recurrences;
b) Regular reviews of the effectiveness of the ISMS shall be undertaken as per the security calendar (GI-ISMS-ENT-003) including meeting security policy objectives and review of security controls. This shall take into account the results of the audits (GI-ISMS-ENT-003), incidents reported on the IMS, suggestions and feedback from all affected parties;
c) Effectiveness of security controls shall be verified by conducting audit and review activities as per the security calendar (GI-ISMS-ENT-003);
d) The RA (F-ISMS-ENT-029) shall be reviewed as per the security calendar (GI-ISMS-ENT-003) schedule examining the residual and acceptable risks taking into account the changes to:
   - Organization;
   - Technology;
   - Business objectives and processes;
   - Identified Threats;
   - Effectiveness of the implemented controls;
   - Any external event likely to affect (e.g. legal and regulatory environment and changes to the social climate).
e) Internal ISMS audits shall be conducted as per IRM Security Calendar (GI-ISMS -ENT-003);

f) Management review of the ISMS shall be undertaken at least once a year ensuring that the scope remains adequate and improvements shall be identified;
g) The security plan shall be updated taking into account the review and monitoring findings;
h) Actions and events that could have an impact on the effectiveness or performance of the ISMS shall be recorded in the form of ISMS records.

4.4.4. Maintaining and improving the ISMS

The following shall be done regularly:

- IRM Team is employed to independently perform the information security assessment and monitor the security controls in the information system on an ongoing basis.
- For any non-conformity (NC), IRM Team, shares the detailed report with all relevant stakeholders.
- All NCs identified as part of assessment by IRM team are monitored and tracked for closure with relevant mitigation actions taken by the respective stakeholders as required.
- The improvements as an outcome of all inputs from Section 4.4.3 shall be implemented;
- Appropriate corrective actions in accordance with Section 10.1 shall be taken;
- The results (of monitoring) and actions (of implementation) shall be communicated to all concerned parties;
- Post implementation review shall be carried to ascertain whether the intended objectives were achieved.

5.Leadership

5.1. Leadership and Commitment

Leadership commitment shall be exemplified by publishing the Security Policy Statement (Annexure D) and by demonstrating the following ways:

a) Establishing an Information Security Policy Manual (this document);
b) ensuring the integration of the information security management system requirements into the organization's processes;
c) Allocating adequate resources for implementation and maintenance of the ISMS;
d) Communicating to all employees of their security responsibilities and Firstsource's security objectives and Intent (by publishing the Security Policy Statement - Annexure D);
e) ensuring that the information security management system achieves its intended outcome(s);
f) directing and supporting persons to contribute to the effectiveness of the information security management system;
g) promoting continual improvement; and
h) Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2. Policy

The ISMS policy shall include the following:

a) Security Policy Manual as per section 4.3 including control objectives;
b) Scope of the ISMS (section 4.3);

c) Supporting procedures, control guidelines and checklists for the ISMS;
d) Risk Assessment methodology description as per section 4.4.1(b);
e) RA report (F-ISMS-ENT-029) as per 6.1.2 to 6.1.3(b);
f) Risk Treatment Plan as part of the RA (F-ISMS-ENT-029);
g) Documented procedures for planning, implementations and operation of the security controls;
h) A Statement of Applicability (SoA, PR-ISMS-ENT-002) listing the applicable controls and justifications for the excluded ones.

5.3. Organizational roles, responsibilities, and authorities

a) Top management shall assign and communicate the responsibilities and authorities for roles relevant to information security to ensure ISMS confirms to the requirement of the ISO 27001 standard;
b) Reporting on the performance of the information security management system to the top management happens at least annually through RISK COMMITTEE (Management Information Security Forum).

6.Planning

6.1. Actions to address risks and opportunities

6.1.1. General

The internal & external issues and requirements of the interested parties that are relevant to the information security management system shall be considered to determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system achieves its intended outcome(s);
b) prevent, or reduce, undesired effects through preventive actions; and
c) achieve continual improvement through PDCA.

Firstsource shall plan:

d) actions to address the risks and opportunities; and:
   - Based on criteria described in section 6.1.2 the level and types of Acceptable (residual) risks shall be described (F-ISMS-ENT-029);
   - Evaluating need for action to prevent occurrences of NC's;
   - Determining and implementing the preventive actions;
e) to
   1. integrate and implement the actions into its information security management system process through:
      - Risk Treatment Plan as part of the RA (F-ISMS-ENT-029);
      - Determining and implementing the preventive actions;
   2. evaluate the effectiveness of these actions through:
      - Follow-up actions from previous RISK COMMITTEE meetings;

6.1.2. Information security risk assessment

Information security risk assessment shall be performed at least once a year as per the Risk Management Policy (PL-ISMS-ENT-008) or when there is a significant change to the information system or operational environment and shall take into account the business information security, legal and regulatory requirements and communicate the results of the risk assessments to the stakeholders and management.

Information security risk assessment shall cover following aspects:

(i) external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously;
(ii) the types of accounts offered by the organization and the methods the organization provides to open and access its accounts;
(iii) knowledge and experiences of incident histories and actual case impact scenarios; and
(iv) systems architectures.

The Policy shall mandate that appropriate control objectives and controls be devised to reduce risks to acceptable levels.

a) the Risk Management Policy (PL-ISMS-ENT-008) shall establish and maintain information security risk criteria that include:
    1) Risk acceptance criteria and the levels of risks that will be accepted;
    2) The RA (F-ISMS-ENT-029) shall be reviewed as per the security calendar (GI-ISMS-ENT-003) schedule examining the residual and acceptable risks taking into account the changes to:
        1. Organization;
        2. Technology;
        3. Business objectives and processes;
        4. Identified Threats;
        5. Effectiveness of the implemented controls;
        6. Any internal or external event likely to affect (e.g. legal and regulatory environment and changes to the social climate).
b) Usage of the RA templates (F-ISMS-ENT-029) shall ensure comparable and reproducible results;
c) Risks Identification
    1) An IT and Support services catalogue (F-ISMS-ENT-026) shall be established and documented;
    2) Threats to the Information Assets shall be identified (F-ISMS-ENT-029);
    3) The Vulnerabilities that could possibly exploit the threats shall be documented (F-ISMS-ENT-029);
    4) The Impacts that losses of CIA are likely to cause shall be documented (F-ISMS-ENT-029);
    5) The risk owners shall be identified as per the IT and Support services catalogue.
d) Risk Assessment
    1) Loss of business that might result from a security failure shall be assessed taking into account the potential consequences of a loss of CIA of the services and data assets;
    2) Realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities and the controls that have been implemented shall be assessed;
    3) The level of risk shall be estimated;
    4) Based on criteria described in section 6.1.2 the level and types of Acceptable (residual) risks shall be described (F-ISMS-ENT-029).
e) Information security risk shall be evaluated to
    1) compare the results of risk analysis with the risk criteria established; and
    2) prioritize the analysed risks for risk treatment.

6.1.3. Information security risk treatment

a) The Risk Treatment options shall be evaluated and selected from amongst the follows:
    1) Appropriate controls implemented;

2) The residual risks shall be identified and accepted as per the criteria established in the Risk Management Policy (PL-ISMS-ENT-008);
3) The Risk shall be avoided if possible as per PL-ISMS-ENT-008;
4) The Risk shall be transferred to other parties (e.g. Insurance, supplier) as per PL-ISMS-ENT-008

b) Control Objectives and Controls shall be identified and documented (ISMS-001) based on the Risk Management Policy (PL-ISMS-ENT-008) and the RA (F-ISMS-ENT-029). Control selection shall take legal, regulatory and contractual obligations into account. Control objectives and controls shall be listed as Annexure A.
c) SoA (PR-ISMS-ENT-002) shall be prepared to include the following:
1) Control objectives and controls selected in 6.1.3.b and the reasons for their selection;
2) Control objectives and controls currently implemented as per 6.1.2.d.2;
3) Exclusion of control objectives and controls listed in Annexure A and their justifications;
d) SoA (PR-ISMS-ENT-002) shall be produced that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of the controls;
e) A Risk Treatment Plan detailing the controls shall form the comments field of the RA (F-ISMS-ENT-029);
f) Risk Treatment Plan as part of the RA (F-ISMS-ENT-029);

6.2. Information security objectives and planning to achieve them

RISK COMMITTEE shall provide security directives to achieve the security objectives at relevant functions and levels as per F-ISMS-ENT-030. The information security objectives shall demonstrate:
a) consistent with the information security policy;
b) measurable (if practicable);
c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
d) communicated through management meetings;
e) updated as appropriate;

The F-ISMS-ENT-030 shall have documented information on the information security objectives and how to achieve them; the below shall also be determined and documented as per F-ISMS-ENT-030:
f) objectives that shall be performed;
g) resources that shall be required;
h) identification of responsible stakeholder;
i) timelines for the completion shall be determined and documented;
j) method of evaluation for the intended results.

7.Support

7.1. Resources

Firstsource shall determine and provide resources and ensure that resources are available for expenditure as planned for the following:
a) Establish, implement, operate and maintain the ISMS;
b) Ensure that the security procedures support the business requirements;
c) Identify and address the legal, regulatory and contractual security obligations;

d) Maintain adequate security by correctly implementing the identified controls as per the SoA;
e) Carry out internal and external audits and to implement the recommendations arising thereof;
f) Action changes that shall improve the effectiveness of the ISMS.
g) Annual maintenance costs for all the critical products to support and review the ISMS;

7.2. Competence

Firstsource shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

a) Identifying the competencies required for the ISMS tasks;
b) ensure that these persons are competent on the basis of appropriate education, training, or experience;
c) ensure that senior security officials responsible for information security have received appropriate information qualification/certifications or has gained a minimum of five years of role-related experience;
d) Provide the necessary training or hiring people with the required competencies as per the Job descriptions for various roles and evaluate the effectiveness of the training provided;
e) Maintaining records of training, skills, certifications, etc.

7.3. Awareness

Firstsource shall ensure that all personnel are aware of the following through appropriate information security awareness trainings:

a) the information security policy;
b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance;
c) the implications of not conforming to the information security management system requirements.

Security briefings shall be provided to all the employees to make them aware of their security responsibilities and its role in achieving successful ISMS.

7.4. Communication

Firstsource shall determine the need for internal and external communication relevant to the information security management system:

a) the content of the communication shall be relevant and appropriate;
b) the communication shall go out at appropriate time;
c) the communication shall be communicated to required stakeholders (internal and/or external); all public communications are performed by corporate communications team; client relationship managers are responsible to communicate with the clients;
d) the communication channels shall be over e-mail or phone or processes approved by corporate communications team.
e) The public shall have access to information about the organization's security and privacy activities and shall be able to communicate with its DPO/Privacy officer.
f) Firstsource Security and Privacy activities shall be uploaded on the Firstsource company website. It shall be available on below link https://www.firstsource.com/privacy-policy/
    - The public will be able to communicate with its senior security official and senior privacy official and any query can be mailed to - marketing@firstsource.com

7.5. Documented information

7.5.1. General

The ISMS documentation shall include the following:

a) Security Policy Manual as per section 5.2.a including control objectives;
b) Scope of the ISMS (section 4.3);
c) Records generated as an outcome of the operations of the security controls;
d) A Statement of Applicability (SoA) listng the applicable controls and justifications for the excluded ones (PR-ISMS-ENT-002);
e) Supporting procedures, control guidelines and checklists for the ISMS;
f) Risk Assessment methodology;
g) RA report (F-ISMS-ENT-029);
h) Risk Treatment Plan as part of the RA (F-ISMS-ENT-029);
i) Documented procedures for planning, implementations, and operation of the security controls.

7.5.2. Creating and updating

Firstsource shall ensure when creating and updating ISMS documented information is as per Document Control Procedure (PR-ISMS-ENT-001):

a) identification and description of the document created or updated;
b) format and media;
c) Adequacy vis-à-vis the Policy reference and periodic review with an authorized change process.

7.5.3. Control of documented information

The ISMS documents shall be protected and controlled as per the Document Control Procedure (PR-ISMS-ENT-001) which shall take the following into account:

a) Adequacy vis-à-vis the Policy reference;
b) Periodic review with an authorized change process;
c) Changes and current revision status identified;
d) Only the latest version available to authorized personnel;
e) A master list (F-ISMS-ENT-001) shall be maintained to easily identify the documents;
f) Access authorization and information storage, handling, transmission and disposal is as per the classification assigned;
g) External Documents (e.g. Legal, Client Contract, Third party agreement) should be clearly identified and documented;
h) Distribution of documents shall be controlled;
i) Obsolete documents shall be protected from accidental access/usage;
j) Obsolete documents shall have unique nomenclature;

All ISMS records shall be controlled in terms of distribution and access. An ISMS Records List shall be maintained for easy identification and retrieval. Controls shall be implemented to ensure identification, storage, protection, retrieval, and retention period and secure disposal. This shall include records pertaining to security incidents.

8.Operation

8.1. Operational planning and control

Firstsource shall plan, implement, and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. Operations shall be managed as per various procedures listed in the Master List (F-ISMS-ENT-001).

All ISMS records shall be controlled in terms of distribution and access. An ISMS Records List shall be maintained for easy identification and retrieval. Controls shall be implemented to ensure identification, storage, protection, retrieval, and retention period and secure disposal. This shall include records pertaining to security incidents.

All changes (including information processing facilities, applications, software, operating system) shall be processed via the CMS application (Change management System) as described in PR-ITSM-ENT-113 (external document to the ISMS). All applications shall be reviewed from a functions and security perspective after any operating system changes prior to releasing on the production computers as per the release management procedure PR-ITSM-PDM-114 (external document to the ISMS). Appropriate procedures and controls (GI-ISMS-ENT-002) shall be implemented to enable prompt detection and response to security Incidents.

Firstsource shall ensure that security controls and service levels defined in the 3rd party or outsourced service delivery agreements, are implemented, operated, and met. All third parties who handle Business data shall be audited at least once a year to verify that the security controls and service delivery levels specified in the third-party agreements are being met; the service levels shall be monitored by the respective process owners at Firstsource. All changes effected for maintaining and improving the third-party services, shall be managed by way of ensuring that approval from the process owner at Firstsource is sought, prior to implementing the change. The process owner shall ensure that the changes are appropriately timed to ensure minimum business disruption. All outsourced software development shall be managed via contracts that must include service delivery and security clauses.

8.2. Information security risk assessment

The RA (F-ISMS-ENT-029) shall be reviewed at least annually or when significant changes are proposed to occur, as per the security calendar (GI-ISMS-ENT-003) schedule examining the residual and acceptable risks taking into account the changes to:

a) Organization.
b) Technology;
c) Business objectives and processes.
d) Identified Threats.
e) Effectiveness of the implemented controls.
f) Any internal or external event likely to affect (e.g. legal and regulatory environment and changes to the social climate).

The results of the information security risk assessment shall be documented and retained as per the RA report (F-ISMS-ENT-029).

8.3. Information security risk treatment

The Risk Treatment Plan shall be implemented, and their progress be tracked.

Risk assessment & treatment records shall be documented, retained, and controlled in terms of distribution and access.

9.Performance evaluation

9.1. Monitoring, measurement, analysis, and evaluation

ISMS monitoring procedures shall be implemented to determine:

a) effectiveness of the selected controls measured as per the criteria described against each control in Annexure A; action to be initiated upon the measurement values shall also be defined in Annexure A;
b) the method for monitoring, measurement, analysis and evaluation shall be as per IRM - Audit Manual (external document);
c) frequency for the monitoring and measuring shall be as per IRM Security Calendar (GI-ISMS-ENT-003);
d) RISK COMMITTEE shall monitor and measure.
e) Regular reviews of the effectiveness of the ISMS shall be undertaken as per the security calendar (GI-ISMS-ENT-003) including meeting security policy objectives and review of security controls. This shall take into account the results of the audits (as per I-ARM (Internal Audit and Risk Management) ISA - Audit Manual, external document), incidents reported on the IMS, suggestions and feedback from all affected parties;
f) IRM team shall analyse and evaluate the results as per the security calendar (GI-ISMS-ENT-003) .

9.2. Internal audit

9.2.1 General: Firstsource shall conduct internal audits as per IRM Security Calendar GI-ISMS-ENT-003.

9.2.2 Internal Audit Program: Internal audits shall be performed to determine that the control objectives, controls, processes, and procedures conform to the following:

a) ISO/IEC 27001 Standard and all applicable legislations and regulations (including client contractual obligations and all acts, laws or regulations that apply to its clients, e.g. DPA, HIPAA, GLBA, etc. This shall be as per the Global Regulatory Compliance Policy (external document) maintained by Compliance and legal);
b) Industry best practices, vendor recommendations and Firstsource Information Security team specifications;
c) Effectively implemented and maintained;
d) Perform as expected (by way of defined baselines that shall be part of the ISMS documentation.
e) The IRM Security Calendar GI-ISMS-ENT-003 - shall take the importance and sensitivity of the processes and previous audit results into account and appropriately define the frequency and coverage of the audit activities;
f) The audit criteria, scope, frequency and methods shall be defined in IRM Security Calendar GI-ISMS-ENT-003. Selection of auditors and conduction of audits shall ensure objectivity and without bias. Auditors shall not audit their own work;
g) The responsibilities and requirements for planning and conducting audits, reporting and maintaining records, shall be defined in the IRM Security Calendar GI-ISMS-ENT-003 - Audit Manual (external document);

Process and asset owners shall ensure prompt redress of non-conformities and their root causes. Follow-up and verification of closure shall be reported and documented to ensure improvement as described in section 10.

9.3. Management review

The RISK COMMITTEE shall review the ISMS at least once in a year checking for suitability, effectiveness and adequacy. The review shall examine the policies and security objectives. Results of reviews shall be documented.

The management reviews (RISK COMMITTEE and Compliance Reviews) shall include consideration of:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management system;
c) feedback on the information security performance, including trends in:
   1) nonconformities and corrective actions;
   2) monitoring and measurement results;
   3) audit results; and
   4) fulfillment of information security objectives;
d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

10. Improvement

10.1.Continual improvement

a) Firstsource shall continually improve the effectiveness of the ISMS through one or more of the below:
   - Security Policies
   - Procedures;
   - Security Objectives (as per F-ISMS-ENT-030);
   - Audit results;
   - Analysis of monitored events;
   - Corrective actions initiated;
   - RISK COMMITTEE Reviews
b) The improvements as an outcome of all inputs from Section 4.4.3 shall be implemented;
c) Post implementation review shall be carried to ascertain whether the intended objectives were achieved.
d) Action changes that shall improve the effectiveness of the ISMS.

10.2.Nonconformity and corrective action

Firstsource shall take following steps when nonconformity occurs:

a) close the nonconformity, and as applicable;
   1) take action to control and correct it; and
   2) deal with the consequences;
b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;
c) implement any action needed;
d) review the effectiveness of any corrective action taken; and
e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Firstsource shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken, and

g) the results of any corrective action.

Annexure A

Control Objectives and controls

A.5 Organizational Controls

A.5.1 Policies for information security

Shall be approved by management and published and communicated to all employees and relevant external parties. Shall also retain the responsibility for its cybersecurity program in compliance with applicable regulatory requirements.

A.5.2 Information security roles and responsibilities

All information security responsibilities shall be clearly defined. They are as follows: All information security responsibilities, risk designations to all organizational positions as required shall be clearly defined, establish required screening criteria, review and revise designations annually. They are as follows: The **CEO** shall be the top Management's interface for all security directives. The CEO chairs the RISK COMMITTEE and shall be the final escalation point for all Level 3 Incidents. The CEO also signs the Information Security Policy Statement (Annexure D), which represents Firstsource's commitment to Information Security.

Head - Technology authorizes new Information facilities and change to the existing infrastructure as per the Change Management Procedure (PR-ITSM-ENT-113, external document to the ISMS). All level 4 and 5 incidents shall be escalated up to the head technology. The head technology shall be the Owner of all Technology assets and related documents. He/she shall be the final escalation point for all technology related issues including availability of systems.

Head - IRM oversees the logical security at Firstsource. Firstsource shall formally appoint a qualified Head IRM, reporting to senior management, and who is directly and fully responsible for the privacy of covered information. The Head-IRM has direct access to the CEO & MD for Security related issues; for day-to-day functioning and within the management structure. The data protection officer/ Head IRM shall be responsible for the Firstsource's individual privacy protection program, and such appointment is based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill required tasks. Responsibilities include:

• Defining the security framework for the organization;

- Developing, maintaining, updating and approving (on behalf of RISK COMMITTEE) the information security and Privacy policies and Procedures.
- Drawing up annual security plans identifying top issues and recommend countermeasures;

- Provide leadership to the IRM team whose functions are as described below;
- Advising the RISK COMMITTEE on Information Security as the SME (subject matter expert) and convening the RISK COMMITTEE meetings.
- Report in writing on Firstsource's cybersecurity program and cybersecurity risks to senior management through compliance review/RISK COMMITTEEs.
- Serve as the point of contact for all privacy-related issues, which would include the below –
  • Dealing with privacy-related complaints received
  • Provide privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed.

- While performing any task, Head IRM would be informed and aware of the risks associated with processing operations. Head IRM shall consider the nature, scope, context and purposes of the processing.
- IRM Head within the organization shall review and approve the security categorizations and associated guidelines. This security categorization and guideline review shall be in line with the ISMS review as per ISMS manual section 4.4.3. If required, changes shall be made to the policy wherever applicable.

Further Firstsource shall ensure below regarding Head IRM responsibilities-

- Responsibilities of Head IRM do not result in a conflict of interests.
- Support Head IRM in performing the tasks required by law or regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations and to maintain the data protection officers expert knowledge. Firstsource will also ensure that the data protection or privacy officer does not receive any instructions regarding the exercise of those tasks, and the officer will be bound by secrecy or confidentiality concerning the performance of those tasks, in accordance with applicable law or regulation.
- Head IRM is not to be dismissed or penalized for performing these tasks.

IRM Team led by the Head-IRM has the following responsibilities:

- Monitor and report the security status of all ISMS processes;
- Processing all Incidents and allocate appropriate levels as per PR-ISMS-ENT-014;
- Provisioning for security training to training team;
- Execute activities of the Security calendar which includes:
  - Technical Compliance Reviews;
- Provide information security clearance to Change Requests;
- Create guidelines and security checklists for all ISMS processes and assets;
- Establish security guidelines for commissioning and de-commissioning of new processes and information assets;
- Evaluation and recommendation of new security solutions;
- Keeping updated on the latest threats, vulnerabilities and security technologies through attending webinars, being registered to various forums. The IRM Team shall not administer any information systems including security devices like firewalls.

HR department has the following responsibilities:

- Implementing the Personnel Security controls (outlined in Section 4.4, ISMS-001);
- Getting all employees to sign the confidentiality agreement (as per the HR process);
- Raising ISAM requests for all new and quitting employees;
- Drafting and maintaining the disciplinary process for security violations in the HR Policies; these polices shall be an external document to the ISMS.
- Establish required screening criteria, review and revise designations annually.

Training department has the following responsibility:

- Arrange for security briefings to be provided to all employees on an ongoing basis (at least once in year) as per guidelines; and also for the security briefings for all new employees prior to their handling any business processes and being granted access to covered information or information systems.
- The training team shall perform at least one training refresher sessions for all employees.
- Training team shall also implement a workforce development program.
- Dedicated security and privacy awareness training is developed as part of the organization's onboarding program, is documented and tracked, and includes the recognition and reporting of potential indicators of an insider threat.

Administration Department, Physical Security and Facilities has the following Security Responsibilities:

- Liaising with Security Guards provider (wherever applicable) to ensure security staff availability;
- Liaising with fire protection provider to ensure timely servicing of equipment;
- Conducting Fire drills regularly;
- Liaising with law enforcement and emergency services (fire, medical, transport) to handle contingencies;
- Configuring Access Cards and recording it in ISAM (Information Systems Account Management).
- Ensure maintenance of DG, UPS and HVAC. All Business, Department heads and Line Managers have the following security responsibilities:
- Implement security policies and directives issued by the RISK COMMITTEE in their work areas;
- Alert HR of any unexplained absence of employees;
- Assist the IRM team in carrying out Risk assessment in their area.
- Get NDA (Non-Disclosure Agreement) signed by all clients being handled by their teams;
- Ensure that all new employees joining their department have had the Security briefing within the 1st month of their joining and make their teams/departments available to attend the periodic security briefings provided by training department.

Technology Operations Team has the following security responsibilities:

- Implement security measures in their Data Centre as per the Firstsource security guidelines;
- Ensure that all systems have the latest patches and fixes applied as per the vulnerability Management Guideline document (GI-ISMS-ENT-014);

- Define and implement a robust backup and restore procedure (PR-ISMS-ENT008) for all critical information in their respective centers;
- Ensure that all vendors and service providers who will be having access to Firstsource IS, have signed the NDA (Non-Disclosure Agreement);
- Allocate and monitor system privileges via ISAM (PR-ISMS-ENT-007);
- Ensure that all external parties including vendors are escorted at all times while working in privileged areas like data center, UPS or DG room, etc.

ENC (Enterprise Nerve Center) have the following responsibilities: The ENC shall function as per the NOC document (external document) and shall be responsible for:

- Monitor the enterprise wide network for availability, performance and errors.

All employees have the following security responsibilities:

- Read, understand and follow the InfoSec Policies Manual (ISMS-001);
- Report any Incident (suspected or actual) to their Line Manager and the central support desk who in turn will enter the incident details in the IMS (Incident Management System) as per PR-ISMS-ENT-014;
- Abide by the Do's and Don'ts (GI-ISMS-ENT-001) explained during security briefings and posted on the security website;
- Additionally, abide by the security guidelines and policies that shall be provided by the client. This includes all regulatory and legal obligations that the client has specified by way of contract terms.
- All employees must ensure that they have attended the training session organized by the training team;

Security requirements shall be part of Job Responsibilities as per Recruitment Policy (external document) available at the respective HR teams of the respective countries. All contract/3rd Party staff that have access to any Firstsource shall have security responsibilities identical to full time employees. However, all the third party contracts signed shall have the security responsibility as per the Annexure H in the contracts.

A.5.3 Segregation of duties

Segregation of duties wherever feasible, shall be affected. The team that shall audit the IS, shall not be administering any devices. Also, the data safes shall be operated using two locks, the keys of which shall be held by two individuals.

A.5.4 Management responsibilities

The management shall require all employees, contractors and 3rd party users to apply security in accordance with the Firstsource policies and client contractual obligations. This shall be ensured by regular awareness sessions, making the policies available on the intranet and by reminding during pre-process briefings. Contractors are provided with minimal system and physical access only after the organization assesses the contractor's ability to comply with its security requirements and the contractor agrees to comply. The contractor's ability to adhere to and support the organization's security policy and procedures are verified during contractor selection process as per Annexure H.

A.5.5 Contact with authorities

Appropriate contacts with law enforcement authorities, regulatory bodies, security service providers and ISP's shall be established. The respective service or process owners shall maintain such contacts, for e.g., Technology Managers

shall liaise with ISP's and carriers and the Physical Security Managers shall liaise with the local police. Disclosure of logs or other audit trail information may be provided to external organizations only if authorized by the RISK COMMITTEE.

The contact information for such organizations shall be maintained within the Centre BCP document (External document to ISMS).

A.5.6 Contact with special interest groups

Within the organization, all employees shall consult the IRM team on all security matters. Their contact details shall be made available on the intranet security website.

The IRM team in turn, shall be in touch with Security advisory forums and subscribe to Security Advisory lists like SANS, CERT, Security focus, bugtraq, etc. The IPS (Intrusion prevention system) vendor shall be contacted to consult on suspected intrusions.

Email records of such communication shall be maintained as records.

A.5.7 Threat intelligence

Firstsource has partnered with several industry experts to gain regular inputs on Threat Intelligence like Security Scorecard, dedicated SOC Team, endpoint and server EDR service providers. The IRM team thereafter analyses each threat in regard to the Firstsource infrastructure and issues advisories as needed.

Firstsource has a well-established Threat Intelligence program in place. As part of this program Firstsource is working with various partners and leveraging services for:

- Enhanced and continuous visibility of cyber threat landscape including dark web, deep web and the surface web.
- Continuously monitoring of the digital risk footprint of online brands for abuse and initiate takedown of offending websites/ content
- Provide attack surface monitoring to help Firstsource security team build a better understanding of their cyber risk exposure.
- Enhance situational awareness thereby improving our ability to rapidly respond to and contain potential security/privacy breaches before they cause unacceptable business impact.
- Providing incident response and facilitating remediation of data security incidents

Firstsource has outsourced 24*7 SOC Team (Security Operations center) that does the following

a) Security Event Monitoring

- Monitoring and analysis of security events resulting from SIEM rules / use cases
- Provide you with analysis and remedial measures for valid security incidents
- Report on incident ticket status
- Recommend and Co-ordinate solutions/Incident Response (IR), for higher severity incidents

b) Malware Analysis

- Malware analysis when unknown or heuristic malwares are detected.
- Detailed behavioral and static analysis of malware is to be issued

c) Threat advisory
Provide information and analysis related to security advisories received from external agencies like State-CERT, National-CERT, security vendors/OEMs.
d) Threat Hunting
Regular Threat hunting using Microsoft Threat hunting feeds, PwC Threat Advisories, Feeds from Sentinelone XDR and feed from various open sources.
e) Orchestration and Automation (SOAR)

A.5.8 Information security in project management

Implementation of new Information facilities and changes to the existing infrastructure shall be as per the Change Management Procedure (PR-ITSM-ENT-113, external document to the ISMS).

A.5.9 Inventory of information and other associated assets

Inventory of all physical assets shall be maintained as per the Asset Management Procedure (PR-ISMS-ENT-005). Individual shall get approval from management for distribution or movement of any media and the records shall be maintained. All the records of such approvals shall be logged, and maintenance of the audit trails shall be done by Firstsource.

A.5.10 Acceptable use of information and other associated assets

Use of all information and information processing assets shall be in compliance with the Acceptable Use Policy as described in PL-ISMS-ENT-003.
All employees must sign acceptable use agreement before allowed access to information asset. The agreement should state that user actions may be monitored and the employee consent to such monitoring. The same must be part of Joining formalities process which is signed by new hires during induction.

A.5.11 Return of assets

All employees, contractors and 3rd party users shall return all Firstsource assets in their possession or usage upon termination of their employment, contract or agreement and in accordance with the separation policy and procedure (external document).

A.5.12 Classification of information

All Information (including those of the clients that are being handled by Firstsource) shall be classified as per the Information Classification Policy (PL-ISMS-ENT-002).

A.5.13 Labelling of information

This shall be as per the Information Management procedure (PR-ISMS-ENT-015).

A.5.14 Information transfer

All information and software exchange shall be in accordance with the Information management procedure PR-ISMS-ENT-015.
Formal agreements shall be established with clients and other 3rd parties where there shall be a requirement for exchanging software or information on an

ongoing basis. The agreements shall be recorded and maintained by respective service or business owner.

A.5.15 Access control

Access control within the Windows domain shall be as per the Domain Security Policy (PL-ISMS-ENT-005); privileged access shall be requested on ISAM (Information Systems Account Management) application, the process flow describing the controls of this application shall be described in the ISAM Procedure (PR-ISMS-ENT-007). Further, it shall be ensured that users have access only to the data he or she needs to perform a particular function as described in ISAM Procedure (PR-ISMS-ENT-007).

Access to any network resource shall be granted only on a “Need To” basis; all network resources such as servers or telecom switches shall be connected only to the DMZ (demilitarized-zone) as per guidelines described in GI-ISMS-ENT-002 and access shall be controlled by firewalls setup as per the firewall guidelines (GI-ISMS-ENT-011). All server and/or device administration shall be via two-factor authentication, over PAM 360 and privileged accounts to utilize dedicated machines for all privileged tasks or tasks requiring elevated access. Network access to privilege accounts shall use replay resistant mechanisms. PAM360 shall be configured for onetime passwords as multi factor authentication. All Network devices for administrative purpose are accessed via two Factor Authentication / Radius Authentication (AAA).

Physical access provisioning shall be as the Physical security/Facilities policy(external document to the ISMS) managed by the Facilities team.

A.5.16 Identity management

All user account creation and deletion requests shall be routed via the ISAM application as described in PR-ISMS-ENT-007. Individual user accounts shall be created for all users (except for the Trainees who have very limited access) as per the Domain Security Policy (PL-ISMS-ENT-005) to ensure accountability for all account usage. Access to all user accounts shall require an ID and a password. Common ID may only be used if a client insists on doing so; in such cases the residual risks shall be clearly explained to the client. For all new employees, access shall only be provided once the background verification process is complete. New Joining process is including background process is as described in the New-Joining formalities document. Upon user registration, Firstsource shall ensure the users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access. The same shall be a part of the Joining process signed by new hires upon induction as per HR SOP. Firstsource shall maintain a list of all workforce members including individuals, contractors, business partners with access to covered information. The listing shall be the same used by Enterprise team for quarterly user review as per the ISAM Procedure document.
Unauthorized remote connections to the information systems shall be monitored and reviewed at least quarterly, and appropriate action is taken if an unauthorized connection is discovered. Firstsource shall employ automated mechanisms to notify specific personnel upon termination of individuals. This shall be as per ISAM Procedure document where daily headcount reports are sent to account owners.

A.5.17 Authentication information

This shall be as per Password and User Account Policy (PL-ISMS-ENT-006); the controls shall be implemented on the Windows Active Directory as per Domain Security Policy (PL-ISMS-ENT-005). Firstsource shall ensure that passwords are disseminated verbally to all new joiners by the training team during their induction process. This would also ensure that users have acknowledged the receipt of passwords.

A.5.18 Access rights

Control implemented in the ISAM (PR-ISMS-ENT-007) forces review of access rights at least quarterly and at least bi-annually for privileged accounts. Firstsource shall ensure that user's access rights are reviewed after any changes in access due to promotion, demotion, transfers within organization, or termination of employment, or other arrangement with a workforce member ends, or access rights reallocated when moving from one employment or workforce member arrangement to another within the same organization. The review should be covered as part of the SAP process sending daily headcount reports to account managers.

A.5.19 Information security in supplier relationships

All suppliers that have access to any Firstsource shall have security responsibilities identical to full time employees. However, all the third-party contracts signed shall have the security responsibility as per the Annexure H in the contracts.

A.5.20 Addressing information security within supplier agreements

Security requirements as described in the External Party Access Policy (PL-ISMS-ENT-001) must be included in all external party agreements along with the NDA (Non-Disclosure Agreement), prior to allowing access to any Firstsource confidential or restricted information or information processing assets. A list of all the external service providers shall be maintained by Firstsource. All the service providers shall comply with the Firstsource defined information security requirements. Firstsource shall also monitor security control compliance by external service providers on an ongoing basis. Firstsource shall include the specific obligations related to information security and privacy in the formal agreement with external service providers. Agreement shall include expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. These agreements shall be reviewed and updated by legal and compliance team on an ongoing basis by verifying the enforced security controls in the external organization. Firstsource shall also ensure that dedicated port, function and protocol required in getting such external services are identified and documented for all the external services. The same shall be used to protect the Firstsource network by blocking such port, function or protocol in case of any attack. Additionally, at Trichy and Pondicherry, outsourcing shall include selection, monitoring and auditing criteria for the KA (Keying Associates) vendors.

A.5.21 Managing information security in the information and communication technology (ICT) supply chain

Security requirements as described in the External Party Access Policy (PL-ISMS-ENT-001) must be included in all external party agreements along with the NDA (Non-Disclosure Agreement), prior to allowing access to any Firstsource confidential or restricted information or information processing assets.

A.5.22 Monitoring, review and change management of supplier services

All third parties who handle critical and confidential data shall be audited once a year to verify that the security controls and service delivery levels specified in the third-party
agreements are being met; the service levels shall be monitored by the respective process owners at Firstsource.

A.5.23 Information security for use of cloud services

Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements. Cloud Computing policy maintained by IT-Ops team is to be referred for details.

A.5.24 Information security incident management planning and preparation

Firstsource shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. This shall be as per the Incident Management Procedure (PR-ISMS-ENT-014)

A.5.25 The organization shall assess information security events and decide if they are to be categorized as information security incidents.

Information security events shall be assessed and decided as per Incident Management Procedure (PR-ISMS-ENT-014).

A.5.26 Response to information security incidents

Response to information security incidents shall be as per Incident Management Procedure (PR-ISMS-ENT-014).

A.5.27 Learning from information security incidents

The IRM team shall review all incident reports and the RISK COMMITTEE shall discuss all Level 1, 2 and 3 incidents during the RISK COMMITTEE meetings. Incident pattern, behavior, similarities and other trend information shall be discussed and appropriate action initiated to prevent recurrences and to improve the overall security levels.

A.5.28 Collection of evidence

All evidence that is collected, retained or presented shall conform to the Incident Management procedure PR-ISMS-ENT-014 as well as comply with all applicable legal and contractual requirements.

A.5.29 Information security during disruption

This shall be in accordance with the Risk Management Policy PL-ISMS-ENT-008. Continuity plans shall be developed and implemented at every delivery center (External document PR-BCMS-XXX-003, where XXX is the center code) in accordance with the Risk Management Policy PL-ISMS-ENT-008.

A.5.30 ICT readiness for business continuity

Conduction of RA as per F-ISMS-ENT-029 shall be integral to the BCM process and in accordance with the Risk Management Policy (PL-ISMS-ENT-008).
All continuity plans shall have a test schedule defined and shall be tested accordingly; the testing shall be verified by the BCP team as per defined calendar.

A.5.31 Legal, statutory, regulatory and contractual requirements

All applicable legislation, laws and acts (e.g. DPA, HIPAA, GLBA, etc.) applicable to the client operations, shall be followed. This shall be as per the Legal & Compliance Policy and documented in the Global Regulatory Compliance Framework of Firstsource (external document) maintained by Legal Team.

All region-specific legislation shall be identified by the legal consultants to Firstsource HR; the consultant shall verify Firstsource's compliance on an annual basis and as and when new legislation/acts are introduced or changed. A list of all applicable legislations shall be maintained by the respective HR (external document).

Firstsource shall ensure that agreed services provided by a network service provider/manager provided securely and are formally managed and monitored.

- Firstsource shall determine the ability of the network service provider to manage agreed services in a secure way and monitor it
- Firstsource shall ensure that right to audit is agreed by the management
- The security arrangements necessary for particular services including security features, service levels, and management requirements, shall be identified and documented.
- Service level agreements shall be reviewed and signed between the organization and service provider.

A.5.32 Intellectual property rights

All license information shall be maintained and documented by the Technology team; the content management and filtering systems shall be appropriately configured to prevent unauthorized downloading of any programs or other content (GI-ISMS-ENT-012); all USB and CDROM drives shall be kept disabled except on designated and controlled PC's as per the domain Security Policy (PL-ISMS-ENT-005); use of unauthorized and unlicensed software is prohibited as per the Acceptable Use Policy (PL-ISMS-ENT-003).

A.5.33 Protection of records

Records vital to the organization's functioning such as contracts, personnel records, financial information, client/customer information, etc. and existence shall be appropriately protected from loss, destruction, and falsification; copies of such documents shall also be maintained off-site; Security controls such as access controls to be in place as per ISAM Procedure (PR-ISMS-ENT-007), encryption and backup requirements as per Section A.12.3.1 Information backup, and information classification restrictions as per Information Management Procedure (PR-ISMS-ENT-015).

A.5.34 Privacy and protection of personal identifiable information (PII)

All client recommended measures to protect the data shall be implemented as per the geographic regulation; all employees shall sign the confidential agreement.

HR shall ensure that personnel information maintained securely and access shall be granted to authorize personnel only.

Firstsource public systems (corporate website) if collecting personal information, shall ensure that the information is protected and the web pages that allow submission of personal information shall carry a privacy statement as detailed in PL-ISMS-ENT-015.

A.5.35 Independent review of information security

Audits by external auditors shall be performed against the Firstsource Information Security Policies and check for continuing compliance. These audits shall be carried out in addition to internal security audits and those initiated by Board. Firstsource shall further ensure that results of these reviews are reported to the management official/office initiating the review as per Audit Manual. The external audit reports shall be maintained as part of the ISMS document tree and shall be retained for at least three (3) years.

Firstsource shall ensure that results of reviews are reported to the management official/office initiating the review. Firstsource shall ensure that following details are being taken care of as a part of review and report process:

- Firstsource shall ensure that independent auditor reports review results either on emails or Firstsource Infosec team shall schedule meetings with the higher management to brief about audit findings or by any other means (physical evidence by courier, physical walkthrough)
- Ensuring that independent reviews are reported back to the management.
- Results shall be maintained for at least 3 years

A.5.36 Compliance with policies, rules and standards for information security

Internal audits as defined in IRM – Audit Manual (external document) shall be conducted as per the schedule and frequency defined in the IRM audit calendar GI-ISMS-ENT-003 to ensure compliance with Firstsource security policies.

A.5.37 Documented operating procedures

Standard Operations Procedure documents for technology data shall be maintained as per PR-ISMS-XXX-001 and telecom team as per PR-ISMS-XXX-002(where XXX is the center name) to implement the Security Policies mentioned in the InfoSec Policies Manual (ISMS-001). These will be external documents to the ISMS and maintained by IT-Ops team.

A.6 People Controls

A.6.1 Screening

This shall be as per Recruitment Policy / screening methodology (external document) maintained by the respective HR / Recruitment regions. Further, HR Team shall ensure that screening records are sent to Operations Team and all other stakeholders via employee engagement.

A.6.2 Terms and conditions of employment

Terms and Conditions of Employment include Security responsibilities for all employees; this shall be part of the appointment letter / employee handbook; the format and the letters shall be available in Employee Personnel Files.

A.6.3 Information security awareness, education and training

All employees shall undergo the security briefing/training during induction and refreshers at least once in a year and training contents shall be available in the ISMS document tree for the respective regions shall be used to train the employees on security awareness for the respective regions. The Format for “Acceptance of security responsibilities sheet”, Training records and acceptance sheet for security responsibilities shall be available online, if CBT is being used for training.

A.6.4 Disciplinary process

HR teams of the respective regions shall have a documented disciplinary process for violations of the security policies, which shall include termination of employment as an action. Supervisors shall be notified within 24 hours when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction.

A.6.5 Responsibilities after termination or change of employment

Responsibility for terminating or change of employment shall be described in the separation policy and procedure available with HR at respective locations (external document).

A.6.6 Confidentiality or non-disclosure agreements

All employees sign the confidentiality Agreement as per the HR Confidentiality Agreement format and the same shall be available in Personnel files. All external parties including vendors shall sign the NDA (Non-Disclosure Agreement).

A.6.7 Remote working

Remote (external) access to the organization's information assets and access to external information assets (for which the organization has no control) shall be based on clearly defined terms and conditions.

VPN shall be used for encrypting the remote sessions to the internal Firstsource network from unknown networks. All VPN connections shall be secured using strong cryptography to protect the data confidentiality and integrity. Secure Socket Layers (SSL) or Virtual Private Networks (VPN) shall be used for transmission of sensitive information over public / open network.

Access to be allowed only from authorised locations/business specific countries.

Remote access to server and data centres (on prem and cloud)

- All administrators/privileged users (server, database, application, IT infra, Back-up admin) shall use 2 factor authentication(PAM 360) and enforced path via the terminal server to get access to Firstsource IT infrastructure, database and application.

VPN

- Remote users shall use secure VPN to connect to office network with 2 Factor authentication.
- SSL, IPSEC and L2TP protocols shall be used for the secure transmission of the data.
- Protocols for secure Access to Firstsource web apps by external parties shall also be secured using SSL.

A.6.8 Information security event reporting

All incidents shall be reported to the Service Desk Support that enters the details into the IMS (Incident management system) application. IMS shall alert the IRM team to review the incident and assign it a “Level” as described in Incident Management Procedure (PR-ISMS-ENT-014). Employees are made aware of the importance and their liability to report all incidents during security briefings as described in GI-ISMS-ENT-004 and the Do’s and Don’ts (GI-ISMS-ENT-001).

A.7 Physical controls

A.7.1 Physical security perimeters

Physical Security perimeter shall be controlled as per the physical security standard operating procedure (external document) defined by the physical security team at respective locations or geography across globe. All entry and exit controls are defined in the respective SOP documents. Firstsource shall develop and review/update a formal, documented physical and environmental protection policy, reviewed annually.

A.7.2 Physical entry

Physical entry controls shall be implemented as per the physical security standard operating procedure (external document) maintained by the physical security team at respective locations or geography across globe.

A.7.3 Securing offices, rooms and facilities

The building shall be divided into multiple access controlled zones. Access shall be configured only on a “Need To” basis. The access rights can be viewed on ISAM (PR-ISMS-ENT-007). Surveillance cameras monitor all access points.

The Server room and the Telecom room shall be additionally protected by PIN based or biometric Access Control. Appropriate approvals shall be maintained by IT Ops to record any visitor or non-routine employee access.

A.7.4 Physical security monitoring

This will be performed by the Physical Security team in accordance with the Physical Security policy (external document to ISMS).

A.7.5 Protecting against physical and environmental threats

Physical protection against fire, flood, earthquake, explosion, civil unrest and other forms of natural and man-made disasters shall be designed and applied at all locations to include adequate fire-retardant material where applicable, fire detection systems and firefighting equipment that shall be regularly tested. External and environmental threats shall be taken into account when leasing or constructing a building for operations.

A.7.6 Working in secure areas

Surveillance cameras shall be installed within the server and telecom rooms; Wherever CCTV are not installed; a log book shall be maintained detailing the visitors name with data and time stamp and these logs must be reviewed by the facility / physical security in charge once in month. Eating, drinking or smoking shall not be allowed in these areas.

Photographic, video, audio and other recording equipment shall not be allowed in these rooms unless authorized by the Physical Security head.

Any work being done by service providers/3rd parties in these areas shall be always monitored and escorted.

A.7.7 Clear desk and clear screen

All IS users shall ensure that they “clean” their desks prior to leaving for a break and at the close of business every day. All users shall also ensure that covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors. Documents containing covered or classified information are removed from printers, copiers, and facsimile machines immediately; and when transporting documents with covered information within facilities and through inter-office mail.
All PC’s participating in the Firstsource Windows domain shall be configured to activate a password protected screen saver with an idle timeout for production and non-production users as per the Domain Security Policy (PL-ISMS-ENT-005).

A.7.8 Equipment siting and protection

All equipment shall be located within access-controlled area. Server and Telecom rooms shall require a PIN / Bio Readers besides a photo proximity access.
Other rooms housing critical equipment but not visited frequently (e.g. UPS or DG room or diagnostic and configuration ports), may be kept under lock and key and access shall be restricted to authorized user. The rooms shall be accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access. There shall be a proper approval in place for people requiring access to these rooms.
Surveillance cameras shall monitor all such areas (wherever applicable). The outdoor cameras shall have protective housings (wherever installed). Duration and safekeeping of the recordings of cameras shall be as per the Record Safeguarding Procedure (PR-ISMS-ENT-003). The recordings shall be stored for 90 days (at least 45 days online backup and 45 days in backup) or as per client specifications – whichever is greater. The DG shall be inside a locked room (wherever applicable). The only equipment that may not be protected by Access control shall be the Generator (henceforth referred as DG)); access to it shall be monitored using surveillance cameras (wherever applicable). All equipment (except the HVAC and the DG) shall be located in a dust-free, air-conditioned environment. Fire alarms and smoke detectors shall be installed throughout the building.

A.7.9 Security of assets off-premises

Equipment to be hosted, if any, shall be in reputed data centers only. All such equipment shall be installed in racks. The racks shall contain only Firstsource equipment and shall not be shared with others.

A.7.10 Storage media

All media shall be marked and handled as per marking and handling guidelines of the Information Management procedure: PR-ISMS-ENT-015.
Secure erasure of information shall be performed prior to disposing erasable media as per asset decommissioning guidelines GI-ISMS-ENT-013 and shall be disposed as per the Information Management procedure: PR-ISMS-ENT-015.
Back-up information that needs to be transported for off-site storage or any information that needs to be sent on media to the clients shall be encrypted as per the Backup and Recovery Policy (PL-ISMS-ENT-009).

A.7.11 Supporting utilities

Provision for UPS power shall be made for all equipment (except the HVAC, exception - workstation not on generators at United States centers) required for operations. Redundant UPS take care of UPS failures; further, a DG set takes over automatically when the main supply fails. Fuel for the DG shall be stored for 24 hours (wherever applicable). Further redundancy for power shall be planned for in the center BCP document (external document) as per the business requirement.

A.7.12 Cabling security

The cabling shall be done by a reputable firm and as per established cabling standards. The cables shall be routed securely to prevent damage or interception. Power and Data / Voice Cables shall be routed through separate ducts and conduits.

A.7.13 Equipment maintenance

All critical equipment shall be maintained as per the manufactures specifications or be under a maintenance contract. All maintenance schedules and reports shall be documented and records be kept for at least 1 year.
Firstsource shall ensure that maintenance and service are controlled and conducted by authorized personnel in accordance the organization's maintenance program.

- Only authorized maintenance personnel will be allowed to perform repairs and maintenance to the equipment for server room.
- For all locations, work permit shall be requested by vendor and is approved by authorized technology team members for maintenance of server room or restricted areas.
- All the maintenance personnel are escorted by the facility and IT team personnel, wherever applicable.
- Appropriate controls are implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization.
- Post-Maintenance
    - Function checklist is prepared and performed
    - Physical signoff is required by vendor and Firstsource if functions are inline after performing the checks.

A.7.13 Secure disposal or re-use of equipment

All configurations shall be erased before the equipment leaves the premises using a secure erasure tool as per the Asset decommissioning guidelines described in GI-ISMS-ENT-013. Techteam shall also use the secure erasure tool wiping all data prior to re-issuing computers.

A.8 Technological controls

A.8.1 User end point devices

All end point such as Laptops / AIO/ Desktop must be installed with an anti-Malware and EDR (End point thread detection). DNS controls must be put in place. The Disks should be fully encrypted and DLP controls with Block policies must be implemented as per business requirement. The machines should have the latest patches no lesser than N-1(N being the latest release).
Login to the system has to be through Firstsource domain, no local user login to be encouraged.

A.8.2 Privileged access rights

Firstsource shall restrict access to privileged functions and all security-relevant information to pre-defined set of users. Firstsource shall ensure that access is explicitly authorized for below security functions but not limited to-
(i) Setting/modifying audit logs and auditing behavior;
(ii) Setting/modifying boundary protection system rules;
(iii) Configuring/modifying access authorizations (e.g., permissions, privileges);
(vi) Setting/modifying authentication parameters; and,
(v) Setting/modifying system configurations and parameters.

The allocation of all privileged access shall be managed by routing all such requests via the Privileged access request feature of ISAM as described in PR-ISMS-ENT-007 and extends any access requirement only for a further 6 months.
Firstsource shall ensure that privileged accounts shall be formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element of users. Firstsource shall also ensure that respective team track and monitor privilege role assignments as per ISAM Procedure document.
Information systems shall prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards

Firstsource shall restrict access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems to personnel based upon the principle of least privilege and supported through technical controls. All virtualized systems shall be access through PAM application and shall has MFA implemented.

The Firstsource shall implement safeguard to protect its information system's memory from unauthorized code execution.

A.8.3 Information access restriction

Information system and application restrictions shall be implemented on the Active Directory and other UNIX hosts as per business requirements; these special accesses shall be requested and be viewed on the ISAM (PR-ISMS-ENT-007).
Firstsource shall ensure that each and every user is a part of an org Unit at domain level. There shall not be any actions that could be performed without authentication and authorization. Unique Ids shall be allotted to users.
Access rights from an application to other applications shall be controlled as per ISAM (PR-ISMS-ENT-007)

A.8.4 Access to source code

SourceSafe shall be used for protecting and controlling access to all source code held by Firstsource as described in software development policy and procedure documents, maintained by the software team.

A.8.5 Secure authentication

All log-on shall be as per the Account log-on procedure document PR-ISMS-ENT-010.

A.8.6 Capacity management

Servers, network devices and links shall be monitored for usage and availability as per NOC document (external document).

A.8.7 Protection against malware

- Gateway based anti-virus and content inspection and filtering shall be set up to prevent viruses and other malware entering the network as per GI-ISMS-ENT-002. All removable media and CDROM drives shall be disabled as per the acceptable use policy (PL-ISMS-ENT-003) and

implementation shall be done as per domain Security Policy (PL-ISMS-ENT-005).

- Employee Security trainings (GI-ISMS-ENT-XXX) and Do's and Don'ts (GI-ISMS-ENT-001) cover measures to be adopted for virus protection.
- All end point such as Laptops / AIO/ Desktop must be installed with an anti-Malware and EDR (End point thread detection).
- All Windows based server Operating systems must be installed with an anti-Malware and EDR (End point thread detection).
- All Unix / CUBS / FACS /AIX servers must be installed with an anti-Malware and EDR (End point thread detection).
- The Antivirus and EDR must be configured for Auto Updates.
- All Logs must be pushed to centralized servers.
- On Access scan must be Scheduled for all Unix / CUBS/FACS/AIX /Windows OS for every 24hrs.
- Periodic scanning must be performed daily for all Unix / CUBS/FACS/AIX /Windows OS.

A.8.8 Management of technical vulnerabilities

IRM team shall constantly be on the lookout for information regarding vulnerabilities and exploits by way of participating and subscribing to relevant security forums and alerting services. The IPS (Intrusion prevention system) provider shall also communicate all such information to the Firstsource IRM team. The team shall review the information applicability of IS and shall issue security advisories and follow up the patching activity as per the Vulnerability Management guidelines GI-ISMS-ENT-014.

A.8.9 Configuration management

Detailed configuration requirements shall be provided for all new IS; installation and commissioning form part of the order for equipment requiring specialist attention. Acceptance criteria shall be set and satisfied prior to commissioning.

A.8.10 Information deletion

Information stored in information systems, devices or in any other storage media shall be deleted when no longer required as per regulatory and contractual requirements.

A.8.11 Data masking

Data masking shall be used in accordance with Firstsource's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Objective and scope:

Data masking is a technique used to create a version of data that looks structurally similar to the original but hides (masks) sensitive information. The version with the masked information can then be used for various purposes, such as user training or software testing. The main objective of masking data is to create a functional substitute that does not reveal the real data.

Various techniques of data masking:

- Replacing personally-identifying details and names with other symbols and characters
- Moving details around or randomizing sensitive data like names or account numbers

- Scrambling the data, substituting parts of it for other parts from the same dataset
- Deleting or “nulling out” sensitive values within data records
- Encrypting the data to make it infeasible for unauthorized users to access it without a decryption key

The respective Application owners, Functional owners, Data Processors, Data controllers shall implement and maintain appropriate administrative, technical and organizational measures to ensure the confidentiality, integrity and availability of all Data and protect it at all times from corruption, loss, destruction and unauthorised disclosure.

A.8.12 Data leakage prevention

Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.
Data leakage prevention tools should be used to:

- Identify and monitor sensitive information at risk.
- Detect the disclosure of sensitive information.
- Block user actions or network transmissions that expose sensitive information
- Preventing data breaches, exfiltration, or unwanted destruction of sensitive data

Any suspected data leakage incident should be reported immediately and no lesser than 24 hours to security@firstsource.com.

A.8.13 Information backup

All information and software shall be backed up (and when equipment is moved or relocated) and tested regularly as per Backup and Recovery Policy (PL-ISMS-ENT-009). The back-up and restoration frequency, methodology and storage period shall take into account all client contractual obligations.
The respective technology data and telecom team shall maintain the backup and recovery procedures in accordance with the Backup and Recovery Policy (PL-ISMS-ENT-009).

A.8.14 Redundancy of information processing facilities

Availability of information processing facilities shall be as per standard/center specific business continuity plan or as per client specific business continuity plan (wherever applicable).

A.8.15 Logging

All access and usage of the network devices and servers shall be logged and stored in a central database as per the Syslog Configuration Guidelines. All applicable legal requirements related to monitoring authorized access and unauthorized access attempts shall be met. The database of logs shall be maintained in the central Repository.

The Security Operation Center (SOC) administrators shall review system access logs on a Real time basis; the log reports shall be made available as per Syslog Documentation; any suspicious activity (activities violating Firstsource InfoSec policy, procedure, or guidelines) shall be reported to the respective Technology Managers who then raises it as an Incident on the IMS.

All faults shall be logged with the Security Operation Center (SOC) as per Incident Management procedure PR-ITSM-ENT-110 (external document to the ISMS). Helpdesk has fault tracking and history maintenance capabilities. Fault history shall be maintained for at least 6 months.
For the following points Audit Logging and Monitoring Procedure shall be referred.

- Firstsource shall create a secure audit record for all activities, such as create, read, update, delete, on the system involving covered information.
- Audit logs generated by SIEM tool in Firstsource systems. Also, it shall include a unique user ID, unique data subject ID, function performed, and date/time the event was performed.
- Firstsource shall ensure that Logs of messages sent and received are maintained including the date, time, origin and destination of the message, but not its contents
- Firstsource shall retain the audit records of all the systems for at least one year.
- Firstsource shall ensure that information system generates audit records which contain the following detailed information:
    - filename accessed
    - program or command used to initiate the event
    - source and destination addresses.
- Firstsource shall ensure that Information collected from multiple sources is aggregated for review
- Firstsource will make sure that all applicable legal requirements related to monitoring authorized access and unauthorized access attempts shall be met and handled by SOC team
- Firstsource shall monitor the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient and secure state
- Monitoring by SIEM tool shall include privileged operations, authorized access or unauthorized access attempts, including attempts to access deactivated accounts, and system alerts or failures
- Automated systems shall be used to review monitoring activities of security systems (e.g., IPS/IDS) and system records on a daily basis, and identify and document anomalies.
- Firstsource shall ensure that SIEM tool generates the alerts for technical personnel to analyze and investigate suspicious activity or suspected violations.
- Firstsource shall analyze and correlate audit records across different repositories using a security information and event management (SIEM) tool or log analytics tools for log aggregation and consolidation from multiple systems/machines/devices, and correlate this information with input from non-technical sources to gain and enhance organization-wide situational awareness.
- Firstsource shall use an intrusion prevention system managed outside of the control of system and network administrators to monitor system and network administration activities for compliance
- Job descriptions shall define duties and responsibilities that support the separation of duties across multiple users.
- Firstsource shall ensure that Security audit activities are independent.
- The initiation of an event shall be separated from its authorization to reduce the possibility of collusion.
- Firstsource shall identify duties that require separation and define information system access authorizations to support separation of duties; and incompatible

duties are segregated across multiple users to minimize the opportunity for misuse or fraud.

A.8.16 Monitoring activities

Automated systems shall be used to review monitoring activities of security systems (e.g., IPS/IDS) and system records on a daily basis, and identify and document anomalies as detailed in A.8.15.

A.8.17 Clock synchronization

All computers and IP network devices shall synchronize their clocks with a single time source; domain controllers (at strategic location) are configured to synchronize time with external time server(s) and other hosts are configured to synchronize time with the respective domain controllers.

A.8.18 Use of privileged utility programs

System utilities that allow generating network traffic, do port scans or launch attacks shall only be installed and authorized on the IRM team computers. Third parties or auditors may be allowed to use system tools if the Head-IRM approves it. Use of system tools by all others shall be prohibited as per the Acceptable Use Policy (PL-ISMS-ENT-003). Implementation of the Content inspection and filtering (GI-ISMS-ENT-012) prevents downloading of executable from the Internet. Also, the domain security policy (PL-ISMS-ENT-005) implementation via Active Directory shall prevent all others from executing such utilities.

A.8.19 Installation of software on operational system

The software code of the applications shall be controlled and any change to the operational code shall be in accordance with Firstsource's Change Management, PR-ITSM-ENT-113 (external document to the ISMS).

A.8.20 Networks security

Network security controls shall be implemented as described in Network Architecture Security Implementation guideline GI-ISMS-ENT-002.

Firstsource shall ensure that periodic monitoring is implemented to ensure that installed equipment does not include unanticipated dial-up capabilities. This shall be a part of annual vulnerability scans and configuration reviews carried out.

Firstsource shall authorize connections from the information system to other information systems outside of the organization using interconnection security agreements or other formal agreements.

A.8.21 Security of network services

All network services shall have their security controls, service levels and management requirements documented in the network services agreement, whether provided in-house or outsourced.

A.8.22 Segregation of networks

VLAN's and DMZ's shall be employed to segregate networks to conform with Firstsource Network Security Controls Document (GI-ISMS-ENT-002) and to the client security requirements.

Firstsource shall employ VLANs to separate user functionality from Information systems management functionality. Access to these VLANs shall be granted as per the Client/Business requirements

Individual client VLAN/DMZ shall be created as per the client contractual/business requirement to provide logical segregation to each client.

A.8.23 Web filtering

The web filter device/application/service should serve as a method of systems monitoring and a stop-gap for risky internet behavior from any host/user within the network. These standards are designed to ensure employees use the internet in a safe and responsible manner and reduce the risk of a compromise to any host on the network.
Web filtering should be applied to all employees, contractors, vendors accessing web content on Firstsource owned or personally-owned computer or any other workstation connecting to Firstsource network.
Only Business specific URLs are to be allowed. Access to any other non-business specific URL needs to be approved by the respective Function Head and IRM Team with business justification.
No internet to be allowed on servers.
Further details are available in the Domain Security policy(PL-ISMS-ENT-005).

A.8.24 Use of cryptography

Cryptographic controls using strong algorithms shall be implemented to protect confidentiality, authenticity and/or integrity of information transmitted and at rest. For in-house developed applications or software, cryptographic controls shall be implemented in accordance with software development SOP/procedure documents, maintained by the software team.

Cryptographic keys shall be managed to protect against modification, loss, unauthorized use and disclosure, as per A.18.1.5 (Regulation of cryptographic controls) or as per the SOP/procedure document, maintained by the respective technology teams.
For applications managed by software team, cryptographic keys shall be managed as per the software development SOP/procedure documents, maintained by the software team.

Firstsource shall ensure that an inventory of key information is maintained. Also, it shall ensure that cryptographic keying material and programs associated with encrypted archives or digital signatures to enable decryption are only stored for the length of time the records are retained.

- Security keys and certification for the decryption purpose shall be maintained for separate clients for the length of retention period by IT team.
- The keys for all the clients shall be retained for the period of time Firstsource is retaining the client data.

Cryptography and Key Management shall be as per the below:

a) Encryption Strength

- All encryption mechanism implemented shall be as per the industry standard (such as AES 256, 3DES, RSA, etc) per client's contractual requirement;

- The use of proprietary encryption is not allowed for any purpose, unless reviewed and approved by Information Security team;

b) Encryption of data at rest (including desktops, laptops, servers, database, applications, external media, etc.)

- Client data / Confidential data / sensitive information stored on computer system owned by and located within Firstsource network must be protected by at least one of the following:
  - Volume encryption or file / folder encryption;
  - Firewall with access control that authenticate the identity of those authorised individuals accessing the data as per the business requirement;
  - Password protection used in combination with all controls including encryption;

Firstsource shall implement technical means to ensure covered information is stored in organization-specified locations.

- Firstsource shall ensure that covered information is stored only in the servers as per the inventory. Further, GAW File transfer scheduler shall ensure that data is moved between configured inbound and outbound paths.
- The data shall be processed only through the approved application.

Where Firstsource chooses not to encrypt covered information, a documented rationale for not doing so shall be maintained or alternative compensating controls shall be used if the method is approved and reviewed annually by the CISO.
The rationale shall be given by the database admin covering the:

- Risk Assessed
- Reason
- Compensative control for protection
- Backup plan in case of any disclosure

c) Transmission Security

- Firstsource shall formally addresses multiple safeguards before allowing the use of information systems for information exchange.
- Cryptography shall be used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems.
- Stronger levels of authentication shall be implemented to control access from publicly accessible networks.
- Stronger controls shall be implemented to protect certain electronic messages, which includes sensitive information throughout the duration of its end-to-end transport path, using cryptographic mechanisms.
- Firstsource shall ensure that no sensitive information is sent through email, instant messaging or chat
- Firstsource shall enhance the protocols used for communications to address any new vulnerability, and the updated versions of the protocols are adopted as soon as possible.

Firstsources shall ensure that include VPN and User access authorization are implemented in the Firstsource environment. Firstsource shall use FIPS approved mechanism such as AES 256, 3DES based on process requirement during transmission to prevent unauthorized information disclosure.

1) Remote access

Remote (external) access to the organization's information assets and access to external information assets (for which the organization has no control) shall be based on clearly defined terms and conditions.

VPN shall be used for encrypting the remote sessions to the internal Firstsource network from unknown networks. All VPN connections shall be secured using strong cryptography to protect the data confidentiality and integrity. Secure Socket Layers (SSL) or Virtual Private Networks (VPN) shall be used for transmission of sensitive information over public / open network with the latest TLS version.

Access to be allowed only from authorised locations/business specific countries.

Remote access to server and data centres (on prem and cloud)

- All administrators/privileged users (server, database, application, IT infra, Back-up admin) shall use 2 factor authentication and enforced path via the terminal server to get access to Firstsource IT infrastructure, database and application.

VPN

- Remote users shall use secure VPN to connect to office network with 2 Factor authentication.
- SSL, IPSEC and L2TP protocols shall be used for the secure transmission of the data.
- Protocols for secure Access to Firstsource web apps by external parties shall also be secured using SSL.

2) Email

Firstsource shall ensure that email messages are protected using strong cryptographic mechanisms such as end-to-end encryption.

- Email access shall be given to specific employees only based on the business requirement. Email communication shall only be used internally in Firstsource network. For external communication approval from manager shall be needed with business justification.
- For any exceptional external domains shall be whitelisted as needed with approval from Business and information security.
- Policies shall be defined to filter the content coming into Firstsource environment.
- Firstsource shall leverage cloud email security application for protection against email information disclosure.
- Email encryption shall be used to prevent unauthorized disclosure. Emails carrying sensitive information such as PHI , PCI to be encrypted .
- Logs shall be maintained and reviewed for events.

- Suspicious emails shall be quarantined by application to create an isolated environment to handle the malware and domain spoofing shall be used to verify the genuine domain.
- Whitelisting of any domain basis business requirement must be routed through Change Request with approvals from Business, Functional, Technology and Infosec Head.
- Incoming media files shall be blocked after performing inspection of the content.
- Microsoft O365 and Teams are the authorized channels for communication within the organization. All communication channels must be protected by appropriate data loss prevention.
- Any sensitive information (including attachments) required to be shared over email must be protected by encryption.
- All emails must be passed through secure gateway to verify for any malicious, suspicious packets, phishing, malware, URLs, etc.
- Any quarantined and blocked emails required to be released for business purpose needs to be approved by Business, Functional, Technology and Infosec Head.

3. Virtual Private Network

Any connection from outside Firstsource network shall be allowed only from approved Firstsource Business locations through a VPN with 2 Factor authentication. Encryption settings are configured in the VPN application with the latest TLS version.

Firstsource shall ensure that Email is protected using the following:

- Encryption
- Password / Passphrase protection (as per PL-ISMS-ENT-006 - Password and User Account Policy)
- All transactions must be logged and reviewed periodically;

d) Key Management

Key management shall be implemented based on specific roles and responsibilities, and this shall take into consideration the national and international regulations, restrictions, and issues. IT/Software team must maintain a key management procedure covering the following details:

- No key ever appears unencrypted;
- Unique encryption keys shall be used per client process and per external application for data in transit and at rest or in storage;
- Keys shall be changed on periodic basis (at least once in six month or as and when necessity arises) for effective key management;
- Any changes to the key needs to be routed via change management process;
- Administrator should ensure acknowledgement is received from the individuals or the key custodian over an e-mail;

- Keys shall be changed or replaced in case of keys are compromised and shall be reported as security incident;
- Keys shall be securely stored and have access only to the authorised individuals (Application Admin, DB admin and Server admin);
- List of keys and users having access to the keys must be reviewed at least quarterly;
- Use of same encryption keys is prohibited for both production and Non-Production;
- Keys that are transmitted or are sent securely to well-authenticated individuals;
- Keys shall be backed up on quarterly basis in a centralised repository, which can be utilized during retrieval of lost Keys.

e) Key Lost/Compromise Recovery

In an event of key lost or compromise, following steps shall be followed:

- Key owner/custodian shall report all key lost or compromised via incident management system;
- Lost/compromised key shall be revoked immediately;
-]Lost/compromised key shall be destroyed;
- New key shall be generated and shall follow the key management steps.

A.8.25 Secure development life cycle

Applications shall be secured by incorporating controls as specified in software development policy and procedure documents, maintained by the software team. Refer **Annexure K** for details.

A.8.26 Application security requirements

Application services exposed to public network/internet shall be protected through a secure and hardened configuration. Network perimeter shall be protected by implementing network firewall and IPS (Intrusion Prevention System). Network perimeter shall be configured into multiple DMZs or zones as per the Network Architecture Security Guideline (GI-ISMS-ENT-002).

Application access and business information over public network/internet shall be configured at least over secure protocol (e.g. https) and through user authentication. Various technical compliance reviews/activities shall be performed as per the Security Calendar (GI-ISMS-ENT-003).

Firstsource shall implement encryption (e.g., VPN solutions or private lines) and it shall log remote access to the organization's network by employees, contractors, or third-party.

A.8.27 Secure system architecture and engineering principles

Applications shall be secured by incorporating controls as specified in software development policy and procedure documents, maintained by the software team. The development and use of system routines and programs which avoid the need to run elevated privileges shall be promoted.

A.8.28 Secure coding

Secure coding principles shall be applied to software development as detailed in **Annexure L**

A.8.29 Security testing in development and acceptance

The production network shall be firewalled from the development network. Test machines shall be used for checking the stability of new patches before applying on to the production machines.
Detailed configuration requirements shall be provided for all new IS; installation and commissioning form part of the order for equipment requiring specialist attention. Acceptance criteria shall be set and satisfied prior to commissioning.

Firstsource shall ensure that independent acceptance testing proportional to the importance and nature of the system is performed both for in-house and for outsourced development to ensure the system works as expected and only as expected.

A.8.30 Outsourced development

All outsourced software development shall be managed via contracts that must include service delivery and security clauses.

A.8.31 Separation of development, test and production environments

The production network shall be firewalled from the development network. Test machines shall be used for checking the stability of new patches before applying on to the production machines.

A.8.32 Change management

All changes to be made to the information processing facilities shall be processed via the CMS application (Change management System) as described in PR-ITSM-ENT-113 (external document to the ISMS).

All exception to the security policy under the ISMS shall be routed through Change Management System and the exception shall be approved by operations head for processes and the functional head for support functions.

A.8.33 Test information

Selection of test data shall be as per criteria specified in software development policy and procedure documents, maintained by the software team.

A.8.34 Protection of information systems during audit testing

All IS audits shall be in accordance with the system audit procedure PR-ISMS-ENT-004 and the schedule as per the InfoSec calendar GI-ISMS-ENT-003. Internal audits shall be conducted as per the schedule and frequency defined in the IRM team Security Calendar GI-ISMS-ENT-003 to ensure compliance with Firstsource security policies. Care should be taken to ensure minimal impact to either information systems or business disruption.

Annexure B

Information Classification Details

Classification: Firstsource Restricted
Information Owner (IO): RISK COMMITTEE
Information Custodian (IC): IRM team
Authorization List (AL): All employees, existing/prospective clients, Contract Staff, 3rd Parties
Declassify on: Never

Annexure C

Changes since the Last Version (Version 10.1)

Date	Version Number	Changes made
	10.1 to 11.0	1. The InfoSec manual has been rewritten to align with the new ISO/IEC 27001 standards. This has resulted in a few additional controls and redefinition and redistribution of some controls leading to overall improved security. 2. Software development, maintenance and support have been included within the scope of the ISMS
	11.0 to 11.1	1. Annexure H added
	11.1 to 11.2	1. Annexure control A8 & A9 updated with the UK centers HR and physical security procedures.
	11.2 to 11.3	1. Removed RVR from relevant sections as center is decommissioned.
	11.3 to 11.4	1. Updated section A.6.1.2 to include TISF
	11.4 to 11.5	1. Annexure F & G updated
	11.5 to 11.6	Updated few section in the document to include the procedures to support the United States centers
	11.6 to 11.7	1. RISK COMMITTEE meeting schedule changed to half yearly
	11.7 to 11.8	1. Included the salt Lake City in section A.8.1.2 Screening
26th May, 2009	11.8 to 11.9	1. Annexure E (Delivery Centers) updated to include Manila, Philippine center; 2. RISK COMMITTEE meeting schedule changed to quarterly; 3. Annexure F (RISK COMMITTEE Members) updated.
24th Sep 2009	11.9 to 12.0	1. Updated Training, Awareness and Competency 2. Updated vulnerability Management Guideline document (GI-ISMS-ENT-014); 3. Updated Ownership of Assets 4. Updated A.8.1.1 Roles and responsibilities, A.8.1.2 Screening

		5. Updated A.8.2.2 Information Security Education, awareness and training , A.8.2.3 Disciplinary Process 6. Updated A.11.4.1 Policy on use of network services 7. Updated A.15.1.1 Identification of applicable legislation 8. Updated A.15.1.6 Regulation of cryptographic controls
2nd Dec 2009	12.0 to 12.1	1. Annexure E (delivery centres) updated to include Pritech and remove MLR center 2. Included priority of preventive action determination requirement under clause 8.3 Preventive action
12th Jan 2010	12.1 to 12.2	1. Annexure E (delivery centres) updated to include Tek Meadows (TKM) and remove Tidel Park (TDL) center 2. Removed TLD references and added TKM references in A.6.2.3 (Addressing security in External party agreements) and A.12 (Information system acquisition, development and maintenance)
7th June 2010	12.2 to 12.3	1. Updated section A.6.1.1 for RISK COMMITTEE & TISF meeting schedule change from quarterly to at least twice in an year 2. Updated section A.8.13 for personal record & exit interview records to Louisville (LFC) 3. Updated section A.6.2.3 for SLA & NDA records to Louisville (LFC) 4. Updated section A.9.1.1 & A.9.1.2 to update the references for physical security procedures. 5. Annexure E (delivery centres) updated to include Tampa (TMP) and Fort Scott (FSK) centres 6. Removed South America and Argentina center references from the document
23rd Nov 2010	12.3 to 12.4	1. In Section A.15.1.6, mentioned about minimum encryption algorithm as AES 256.
22nd Dec 2010	12.4 to 12.5	1. Removed the references of delivery centre TCY (Vedham Towers, Trichy centre), from the document 2. Included the Raja Complex, Trichy centre, in the document referred as RTC 3. Updated Incident Management Procedure, Change Management Procedure & Release Management Procedure document references
30th May, 2011	12.5 to 12.6	1. Annexure section A.9.1.5 is updated and Annexure E and F are also updated.
19th October, 2011	12.6 to 12.7	1. Removed the references of delivery centre RMZ (Ecospace, Bangalore centre), from the document; 2. Removed RMZ references and updated PTC references in A.12 (Information system acquisition, development and maintenance); 3. Annexure E (delivery centres) updated to remove RMZ (RMZ, Ecospace) centre; 4. Annexure F (RISK COMMITTEE members) updated
12th Dec, 2011	12.7 to 12.8	1. Section 5 is updated with the changes to Management Responsibility; 2. Section 7 is updated to reflect the changes in the management reviews; 3. Annexure F (RISK COMMITTEE members) updated; 4. Annexure E updated to include DTT (Dutta Towers, Vijayawada) centre under certified delivery centres;

21st May, 2012	12.8 to 12.9	1. Annexure E (delivery centres) updated to include LVL (Payer) centre under the certified delivery centre scope; 2. Annexure E (delivery centres) updated to remove KLT (Technopolis, Kolkata) centre; 3. Annexure F (RISK COMMITTEE members) updated.
7th June, 2012	12.9 to 13.0	1. Updated sections 5.1, 7, 8, A.6.1.1 and A.6.1.3 updated to reflect the changes in RISK COMMITTEE responsibilities; 2. Annexure F (RISK COMMITTEE members) updated.
3rd July, 2012	13.0 to 13.1	1. Annexure D updated to replace the Information Security Policy Statement.
10th Sept, 2012	13.1 to 13.2	1. Annexure E updated to include CCH (Claremont Church, Derry) centre under Certified Delivery Centres and remove MLD (4th Dimension, Mumbai) delivery centre; 2. Annexure E updated to include AFZ (Airoli-SEZ, Mumbai) & VTO (Vector 1, Manila) under ISMS-ISO-27001 Framework delivery centers.
11th April, 2013	13.2 to 13.3	1. Annexure E updated to include AFZ (Airoli-SEZ, Mumbai) & VTO (Vector 1, Manila) under Certified Delivery Centres and remove AFZ (Airoli-SEZ, Mumbai) & VTO (Vector 1, Manila) from ISMS-ISO-27001 Framework delivery centers; 2. Annexure F (RISK COMMITTEE members) updated.
7th October, 2013	13.3 to 13.4	1. Annexure E updated to include CAD (Discovery House, at Cardiff) & remove VTO (Vector 1, Manila) from Certified Delivery Centres and remove CAD (Discovery House, at Cardiff) from ISMS-ISO-27001 Framework delivery centre; 2. Annexure F (RISK COMMITTEE members) updated; 3. Annexure G (Security Organization Chart) updated.
10th April, 2014	13.4 to 13.5	1. Annexure E updated to move AIE (Prince Info Park, at Ambattur) & FCM (Fountain Court, Middlesbrough) from ISMS-ISO-27001 Framework delivery centres to Certified Delivery Centres; 2. Annexure E updated to move STS (Miami, FL) from Certified Delivery Centres to ISMS-ISO-27001 Framework delivery centre; 3. Annexure E updated to remove KCT Tech Park, Coimbatore delivery centre, as the delivery centre is decommissioned; 4. Annexure F (RISK COMMITTEE members) updated; 5. Updated internal audit procedure/manual references, as internal audits are now performed by ERM ISA.
5th January, 1015	13.5 to 14.0	1. Updated to re-align the requirement of ISO 27001:2013.
17th June, 2015	14.0 to 14.1	1. Annexure E (Certified Delivery Centers) and Annexure F (RISK COMMITTEE members) updated.
4th January, 2016	14.1 to 14.2	1. Annexure E (delivery centers) updated to remove AIE (Prince Info Park, at Ambattur) centre; 2. Annexure E (Certified Delivery Centers), F (RISK COMMITTEE members) & G (Security Organization Chart) updated; 3. Replaced InfoSec team with IRM team and ERM with I-ARM team, as per organizational changes.

3rd January, 2017	14.2 to 14.3	1. Annexure E (Delivery Centers) updated to include certified delivery center and remove decommissioned delivery center.
30th January, 2017	14.3 to 14.4	1. Section A.13.1.3 (Segregation in networks) to include the requirement to provide logical segregation to client; 2. Section A.18.1.5 (Regulation of cryptographic controls) to include the requirement of unique encryption keys per client process and per external application for data in transit and at rest or in storage.
3rd January, 2018	14.4 to 14.5	1. Obsolete references removed / updated; 2. Annexure E (Delivery Centers) updated
11th May, 2018	14.5 to 14.6	1. Obsolete references removed / updated; 2. Annexure E (Delivery Centers) updated
14th August, 2018	14.6 to 14.7	1. Obsolete references removed / updated; 2. Annexure D, E (Delivery Centers) & F (RISK COMMITTEE members) updated; 3. Section A.12.4.1 (Event logging) and A.18.2.1 (Independent review of information security) updated to include the requirement to retain external audit reports for at least three (3) years.
27th December, 2018	14.7 to 14.8	1. Obsolete references removed / updated; 2. Annexure E (Delivery Centers) updated.
12th June, 2019	14.8 to 14.9	1. Section A.17.1.2 (Implementing information security continuity) updated
29th July, 2019	14.9 to 15.0	1. Annexure E (Delivery Centers) updated; 2. Section A.7.2.2 (Information security awareness, education and training) to capture the updated IS training module/content format numbers.
20th August, 2019	15.0 to 15.1	1. Section A.10.1.1 (Policy on the use of cryptographic controls), A.10.1.2 (Key management) and A.14.1.2 (Securing application services on public networks).
23rd October, 2019	15.1 to 15.2	1. Annexure D (Firstsource Group Information Security Policy Statement) updated, with MD & CEO details.
23rd December, 2019	15.2 to 15.3	1. Obsolete references removed / updated
22nd December 2020	15.3 to 15.4	1. Updated few procedures related to Infosec manual
14th October 2021	15.4 to 15.5	1. Updated ISO 27001 delivery center (Name and Address)
20th December 2021	15.5 to 15.6	1. updated Section A.6.2.2 ;Teleworking 2. Updated section 4.4.3 , 4.4.4 , 9.1, 9.2, A 12.7.1 ; Internal Audits are performed as per the IRM Security GI-ISMS-ENT-003 , Responsibility changed from I-ARM to IRM . 3. 3.Removed all reference to TISF. 4. Approach to ISMS Section 2.b; third party assessments are performed annually (Change from BI-Annually). 5. Section A 7.1.2; Removed outdated process reference to Healthcare centers.

		6. A 7.2.2 – Removed ownership of HR and training team for "Acceptance of security responsibilities" sheet for training. 7. 14.1.2 – Removed reference to corporate office location at Mumbai 8. A 15.1.2 – Removed obsolete reference to specific Provider business practice 9. A 17.1.2 – Removed reference to BCI's Professional practices 10. A 18.1.3 – Removed reference to obsolete document 11. A12.4.1 – Security administrators replaced by SOC team and real time instead of daily basis Changed Audit log retention to 1 year. 12. Updated Annexure F. 13. Updated Annexure G.
03rd November 2022	15.6 to 15.7	1 – Updated Annexure C. 2 – Updated Annexure E. 3 – Updated Mexico in all the in-scope locations.
5th January 2023	15.7 to 15.8	1. Renamed the document from ISMS Manual to Cyber Security Policy 2. Renamed MISF references to Risk Committee 2. Made modifications to email requirements 3. Made modifications to Remote Login requirements
20th September 2023	15.8 to 15.9	Updated Annexure D reflecting new MD and CEO's signature on the policy statement
30th November, 2023	15.9 to 16.0	• Updated Annexure E to reflect updated list of ISO 27001 certified centers. • Added Annexure K (Secure Software Development Framework) and Annexure L (Secure Coding Practices) under A.14.1.1. • Removed reference of ISMS from BCP documents to BCMS
28th August 2024	16.0 to 16.1	• Changed the version of ISMS from ISO 27001:2013 to ISO 27001:2022 • Added new controls for Data Masking, Data Loss Prevention, Web Filtering and Cloud computing.
7th January, 2025	16.1 to 16.2	• 1. Added new Geo to scope • 2. Made minor changes to A.6.3 • 3. Replaced Portwise references with PAM 360

Annexure D

RP - Sanjiv Goenka Group
Growing Legacies

firstsource

FIRSTSOURCE GROUP INFORMATION SECURITY POLICY STATEMENT

Information Systems[1] (also referred to as IS) are important business assets. The purpose of this policy statement is to ensure Confidentiality[2], Availability[3] and Integrity[4] of all of Firstsource's Information Systems and to manage Residual Risks, if any. Firstsource recognises IS Security to be a business enabler and is committed to adhering to the specifications laid down in the ISO/IEC 27001 Security Standards, which it has adopted as its security framework.

It is Firstsource's policy to ensure that:

- Availability of all IS and supporting services will be maintained as per contractual obligations
- Information Systems will be protected against unauthorised access[5]
- Confidentiality of information will be assured
- Integrity of Information will be maintained
- All ISMS Information will be Classified[6]
- Only Authorised data will be Encrypted[7]
- Regulatory and legislative requirements will be met[8]
- Business Continuity plans will be produced, maintained and tested
- Information Security training will be provided to all staff[9]
- Viruses, unauthorised and other malicious software will be detected and prevented
- All Security Policy violations and security weaknesses or threats, actual or suspected, will be reported to and investigated by the Head - Information Security

Network activity including Internet browsing and emails may be monitored; Desktop Computers and other IS may be examined for unauthorised content.

Security policy violations may result in disciplinary action leading up to termination of employment and/or criminal prosecution.

Detailed Policies and Procedures exist to support this Policy Statement, which are uploaded on http://security.firstsource.com. For any queries, write to security@firstsource.com

The Information Risk Management Head has the direct responsibility of maintaining the Policy, reviewing it annually and providing guidance on its implementation.

All managers shall be directly responsible for implementing the Policy within their business areas, and for adherence by their teams. All business requirements for availability of Information and Information Systems will be met while ensuring compliance with this Policy. It shall be the responsibility of each employee to adhere to this Policy.

Ritesh Idnani
MD & Chief Executive Officer
Date: September 20, 2023

iRM
CONFIDENTIALITY | INTEGRITY
AVAILABILITY | PRIVACY

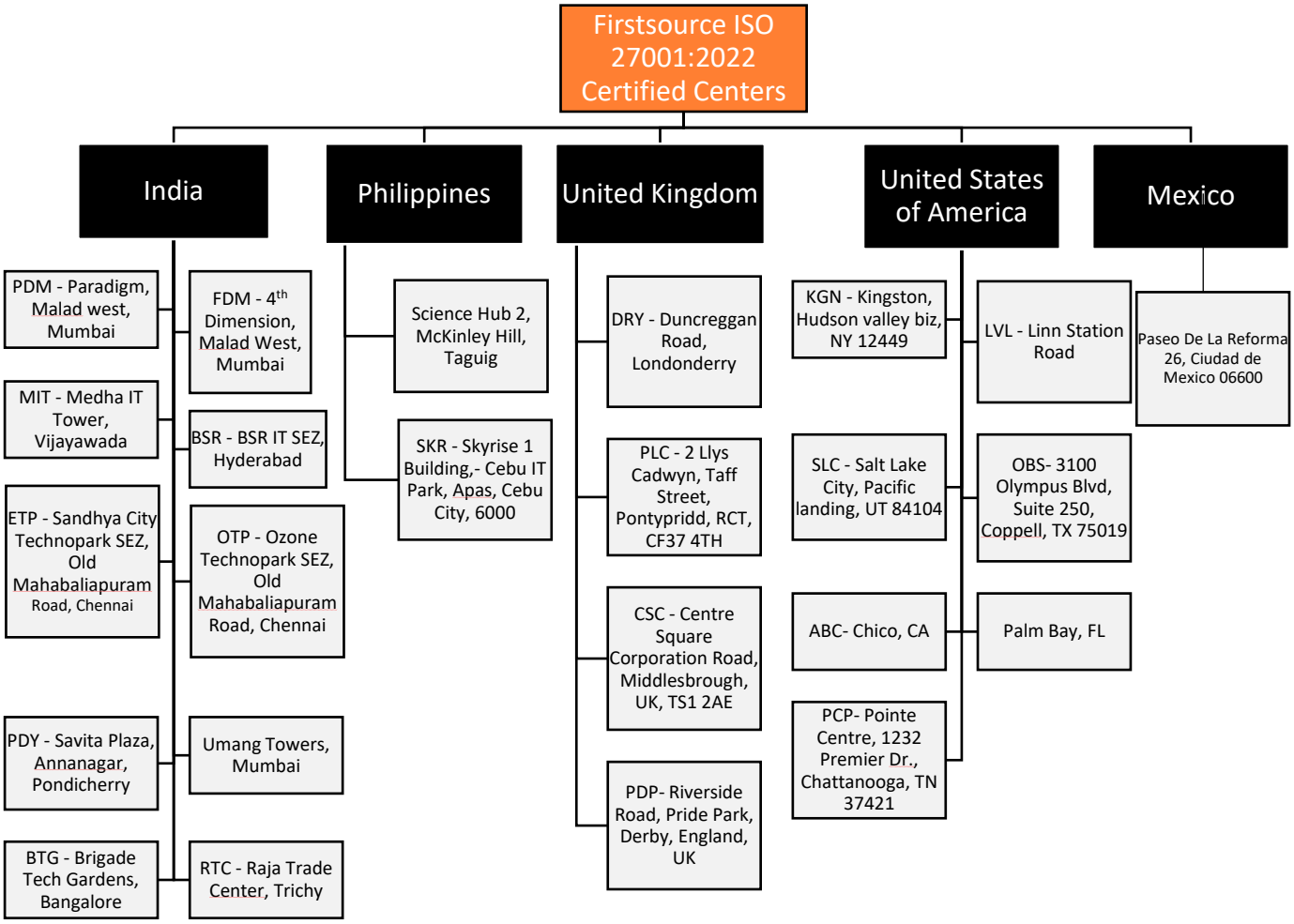
1. Including, but not limited to. Computer hardware. Software, processes, data in all forms of storage, reproduction and transmission.
2. Protecting information from unauthorised disclosure via, but not limited to, email, file transfer or voice conversation.
3. Including System. Application and Data Availability and protecting against Denial of Services attacks.
4. Safeguarding the accuracy and completeness of the information by protecting against unauthorised modification.
5. Anything not explicitly authorised shall be to be treated as unauthorized, access includes physical as well as over any transmission media.
6. Client Information will also be Classified and protected as Firstsource's own Information.
7. Encrypted data includes encrypted files or email. Unless explicitly authorised, data shall be not to be encrypted.
8. To avoid breaches of any criminal or civil law and statutory, regulatory or contractual obligations and of any security requirements.
9. The training content and extent will depend on the role the staff plays in the Company and the projects he or she is associated with.

Report All Information Security Breaches @ http://itsm.firstsource.com/SelfService/

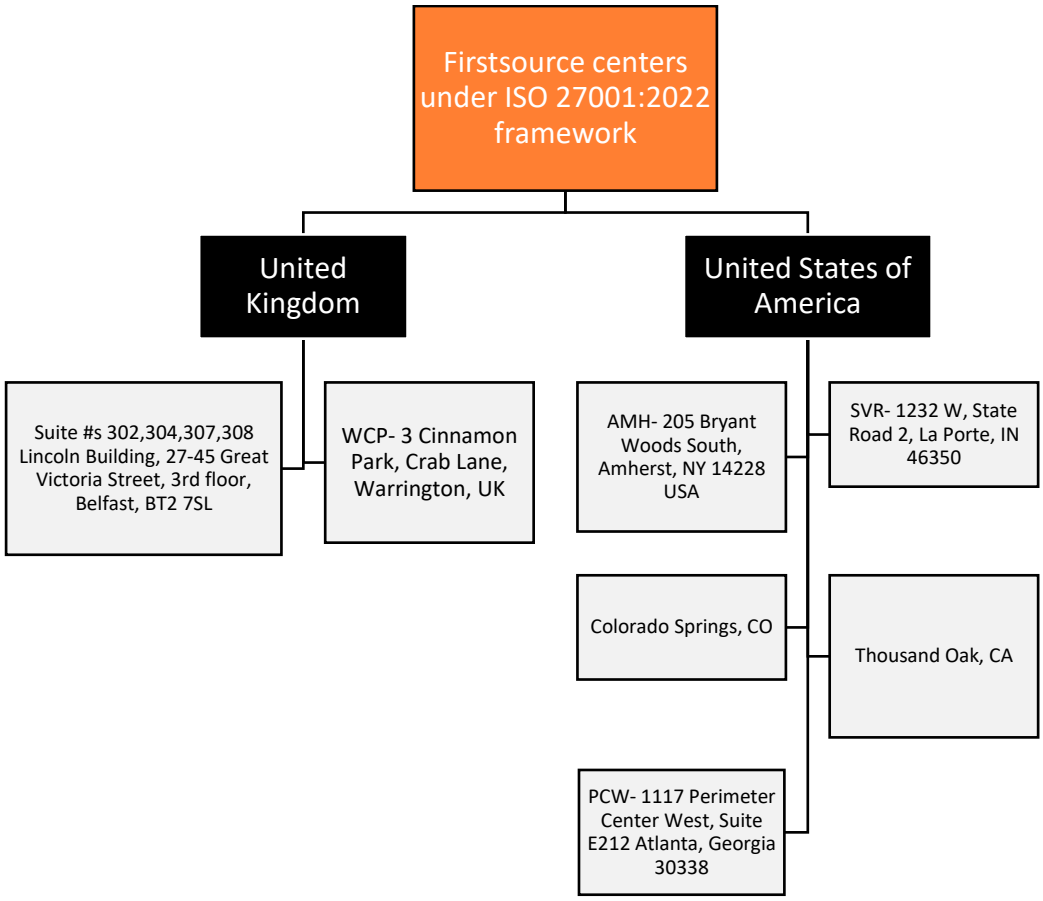
 1

Annexure E

Certified Delivery Centers



Delivery Centers under ISO 27001:2022 Framework



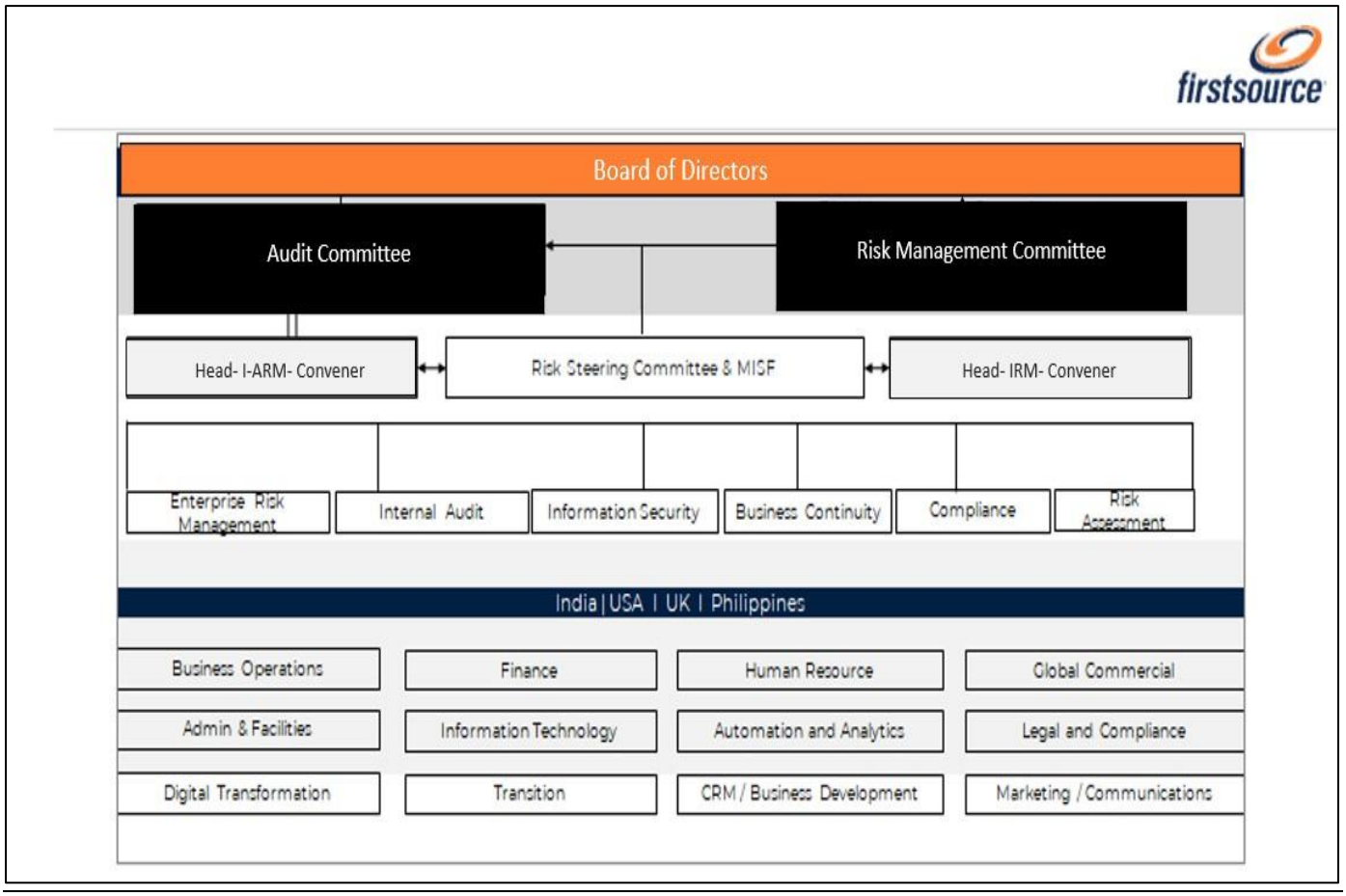
Annexure F

Management Information Security Forum (RISK COMMITTEE) Members

1. Managing Director and Chief Executive Officer - **Chairperson**
2. Chief Financial Officer
3. Chief Human Resources Officer
4. Chief Operating Officer
5. President – Healthcare & Life Sciences
6. President – CMT & Emerging Geos
7. President - Collections & Customer Management (US)
8. Head - Enterprise Transformation Office
9. Chief Administrative Officer
10. SVP - Head of Internal Audit & Risk Management
11. EVP – Finance Controller and Head of Legal & compliance
12. President and Chief Digital Officer
13. Chief Information Officer
14. SVP - Information Risk Management – **Convener**

Annexure G

Security Organization Chart



Annexure H

Security Requirements for Third Party and Vendors

All the third Parties and vendors shall be aware and abide to the following Security Policies defined by Firstsource Solutions Limited:

1. Acceptable Use Policy;
2. Information Classification Policy;
3. Security Do's and Don'ts.
4. External Parties Policy;
5. Incident management policy;
6. Asset Management Procedure;
7. Information classification Policy;
8. Adhering to the HR policies;
9. Procedures followed at Firstsource;

All the third parties and vendors shall the sign the acceptance to adhere to the policy and also confirm to the attended/viewed the following Security Information:

1. Security Policy Statement;
2. Security Responsibilities;
3. Security Briefing.

All third parties and vendors shall read and understand their security responsibilities and shall ensure Firstsource maintain the Confidentiality, Integrity and Availability of its own and its clients' Information and Information Systems and also sign the Non-Disclosure Agreement defined by Firstsource as per their SLA.

Additional Security Requirements of all the IT and Telecom vendors are as below:

- Implementations of the desktop as per the project design;
- Desktop/workstation hardening as per the hardening guideline;
- Backup and restoration as per the backup and restoration procedure;
- Security patching of the servers, workstation and network devices as per the vulnerability assessment process;
- Classification of the information, Information asset as per the process defined under the ISMS;
- Asset Register updating and maintain the asset;
- BCP test as per the test plan / schedule;
- Adhering to SLA as mentioned in the contracts;
- Implementing the mobile computing as per the mobile computing policy;

Additional Requirements for Facilities and BMS Vendors are as below:

- Creation of user ID and providing physical access as per ISAM request;
- Daily maintenance of the access control, CCTV systems;
- Monitoring of the mobile detectors;
- Prepare reports and classify the reports as per the information classification policy;
- Daily test of the UPS, DG and maintain report as mentioned in the ISMS and classify the report as per the information classification policy.

Annexure I

Internal & External Issues

Internal Issues:

- Structure of the organization
- Roles within the organization
- Availability of reliable qualified and competent work force
- Stability of work force
- Staff retention
- Impact of unionization
- Staff training levels
- Contractual arrangements with customers
- Payment terms from customers
- Solvency of customers
- Expansion of customer base
- Overall strength of business to support funding needs

- Opportunities to improve technology e.g. leasing of equipment
- Power consumption
- Data Centre capacity (physical and environmental)
- Resilience of infrastructure
- Relationship with investors
- Credit terms available
- Service level agreements with customers
- Culture within the organization

External Issues:

- Political, economic, social, technological, legal and regulatory
- Environmental e.g. power consumption, recycling or destruction of equipment etc.
- Overall economic performance in the country
- Economic plans for future
- The nature and impact of economy on hosting market
- Customer demographic
- General levels of consumer confidence
- Growth of outsourcing business
- Competitive environment – overall low cost of entry into the market
- Customer expectation
- Standardization and certification within the industry
- Fuel prices - international pressures, domestic market pressures, government taxation regime, etc.
- Regulation within the industry generally
- Licensing requirements in respect of software
- Trade associations and lobbying powers
- Impact on neighbors

Annexure J

Interested parties and need & expectations of interested parties

#	Interested Parties	Needs & Expectations
1.	Employees	Secure & hygiene working environment; Opportunity to grow within the organization; Timely salary; Adequate training to perform the required job.
2.	Clients / Customers	Security of information shared; Abide by legal and regulatory requirement; Abide by contractual obligations; Accurate and timely service, as per the SLA; Economical working.

3.	Shareholders / Board of Directors	Business growth & expansion; Organization profit.
4.	Government agencies/ regulators	Maintain safe working conditions; Co-operate with law enforcement agencies.
5.	Suppliers and partners	Agreement with service details; Timely money for the service performed; Support to the agreement and SLA.
6.	Emergency services (e.g., fire fighters, police, ambulance, etc.)	Co-operation during emergency situations or otherwise; Openness in sharing required information.
7.	Employee families	Secure & hygiene working environment; Opportunity to grow within the organization; Timely salary;
8.	Media	Accurate and timely information; Communication as per the organization policy.

Annexure K

Secure Software Development Framework

Secure Software Development Frame

Annexure L

Secure Coding Practices

Secure Coding Practices.pdf