Global Policy - Physical Security and Safety

Master List Ref	Release Date	Review Date	Next Review Date
Global/Corp/PhySec/POL/001	December 2021	November 2022	January 2025
Version:	**Process Owner**	**Reviewed by**	**Approved by**
1.1	Physical Security	Global Admin Team	CAO

Index

1. Policy Statement

Firstsource Solutions Limited ("Firstsource") has global footprints in India, USA, UK, and Philippines. Firstsource is committed to provide a reasonably practicable security management solution to ensure the security and safety of its employees, contractors, visitors, Firstsource assets and the premises / facilities. Firstsource will take all reasonable steps to ensure that the company is fully secured from any possible foreseeable external as well as internal security threat. Firstsource will ensure the implementation, monitoring, and maintenance of all security measures to: -

- Maintain safe and secure environment in the premises.
- Protect the employees, contractual and service provider staff and visitors within the Firstsource premises.
- Ensure security of the site infrastructure, equipment, materials, and property.
- Provide reasonable security to Firstsource personnel during travel in Firstsource vehicles/ Firstsource service provider vehicles and other logistics, when requisitioned.
- Reduce safety and security incidents thereby achieving unhindered operation and business continuity
- Impart security awareness and training as necessary to Firstsource personnel to enable an incident–free and secured working environment.
- Ensure that all implemented procedures and installed security systems are designed to support business in an effective and efficient manner.

2. Aim

To:

- Lay down the Policy and the guidelines for the security management of a Firstsource facility, personnel, assets, properties, information, and the business operations.
- Facilitate a structured security organisation for Firstsource
- Provide a reference document for the management of the security personnel with necessary guiding principles towards achieving their pursuit of delivering a comprehensive security solution.

3. Scope

This Policy is a living document and therefore sensitive and responsive to the evolving needs of the company and the changing and evolving global threat environment. The Policy is applicable to all Firstsource employees, contractual staff, service providers and visitors of Firstsource. The Policy would be reviewed by facility heads of each geography every year and/ or as the prevailing environment necessitates. Changes to the Policy will be approved by the CAO. The Policy will encompass:

- Physical Security
- Employees
- Visits and Visitor Management
- Information (Proprietary and Confidential) and any other information belonging to and/ or within Firstsource
- Assets and properties
- Operations
- Clients and service providers

The successful implementation of this Policy requires complete commitment from all Firstsource employees at all levels, from senior management to associates. Every employee must co-operate with the Company to enable it to comply with these Policy requirements. Each employee of Firstsource should take utmost care of their own security and the security of fellow employees and property of Firstsource.

All employees are expected to know, acknowledge, and adhere to the security policies and the norms. Noncompliance to the Policy may lead to disciplinary actions.

4. Mission Statement

Protect people, enable day to day business needs, secure assets, protect Firstsource brand and reputation and contribute to savings year over year validated by Key Performance Indicators.

5. Policy Exceptions

There are to be no exceptions to this Policy, exception if any, adversely impacting or altering the security will be signed off by the CAO.

6. Core Principles of Security

Firstsource security plan, process and activities must adhere to the following core principles: -

- The security and protection of employees must be the priority of all business activities.
- Prevention and deterrence of adverse events is the key objectives. Preparedness of the security team to handle an incident and their response must be tested regularly for effectiveness. Threat analysis and risk evaluation shall be carried out on a continuous basis.
- All adverse incidents affecting the security of personnel, information, materials, properties, and assets, including but not limited to security breaches and irregularities must be reported, investigated, and recorded. Corrective action must be taken and followed up to improve the overall security posture and the standard.

- Security team will act as a 'business enabler'. Security team must make every effort to minimise the impact of its security measures on the business functions. Delivery of security services must be timely, seamless, and efficient.
- Security team will maintain a compliant environment, in a cost-effective manner by ensuring that programs and processes are in place that will enable Firstsource to comply with all applicable laws, regulations, contract provisions and company policies.

7. Administrative Security

All security plans, policies, procedures, and processes will be established, implemented, maintained, and applied to all the departments/ functions/ processes, within Firstsource. These will provide necessary guidance to all employees about their responsibilities for protecting Firstsource assets, properties, information, and goodwill.

8. Physical Security

Firstsource premises are either standalone premises or are based out of multi-tenant facilities. These facilities will have outsourced physical security guards and E–security systems in place to protect the people, information, premises, and the physical assets. All other security measures will be integrated with physical security measures, thereby developing a protection profile of 'Security in Layers / Depth'.

- Area Classification: All employees have authorized access to the common areas. Access to other areas will be based on their role and responsibilities. Access to the Restricted and Sensitive Areas will be granted only on 'need basis'. Details of the areas identified and categorized as "Common Areas", "Restricted Areas" and 'Sensitive Areas' is as mentioned below:
  - Common Areas
    - Security Reception
    - Main Entrance
    - Locker Room
    - Cafeteria
    - Parking Bay
  - Restricted Areas
    - Process / Operation Floor
    - BMS/ Security Control Room/Facilities Office
    - AHU Room
    - Cafeteria Kitchen
    - DG Set Area
    - Chiller Unit
    - AHU Room
  - Sensitive Areas
    - Data Center / Hub Room
    - Electrical Room

- UPS Room

9. E-Security & Surveillance

Access Control System, CCTV monitoring, fire alarm Systems and other building management systems, a dedicated BMS Room / Security Operations Centre (SOC) will be maintained and manned 24 x 7 for the effective management of the Firstsource premises. CAO must be intimated with immediate effect in case the Access Control System becomes inoperative for three (3) days or more.

- Access Control Backups: Data back-up must be maintained for a minimum of one (01) year and can be off-site as and when required by any Firstsource client.
- CCTV Coverage/ Monitoring and Back Up: The premises will be under CCTV monitoring and or coverage depending on operational needs. The data back-up of the CCTV coverage will be stored / captured within the system and or on an external media as per the service levels indicated by the Firstsource clients: -
    - 90 days storage – within the DVR system inclusive of data available on external media in case of International clients. Offsite storage will only be done if the client SLA requires it.
    - 45 days storage – within the system inclusive of data available on external media in case of Domestic clients.
    - UK – 30 days on-site storage for telecommunications and media client sites and 90 days on site storage for banking client sites.

10. ID Access Cards

With the exception of the UK, the security team will activate, inactivate and or deactivate access through ID Card within twenty-four (24) hours of being requested by internal stakeholders. On all UK sites, this is the sole responsibility of the on-site Facilities Coordinator(s)

11. Access Management

Within the premises, access of employees, trainees, candidates, contractual staff, clients, service provider staff, Client and temporary staff will be controlled and monitored by employing authorized access cards with the defined level of access. Types of Physical Security Cards are as provided below:

- Visitor Card
- Service Provider Card
- Service Provider Photo Access Card
- Candidate Card
- Trainee Card
- Client Access Card
- Employee Access Card
- Employee Photo Access Card
- Client Photo Access Card

- Safety Information Card

- Note: Loss of Card/Access Card will attract a recovery amount as specified in respective Geography SOP. This activity will be managed and accounted for by the Security team.

Access Levels: Access levels will be granted by the Security team basis the ISAM and or process head approval, the 'need to have' as specified in respective Geography SOP. Name of the access levels will be clearly defined in respective Geography SOP.

Sl. No	Name of Access Level	Doors to be given Access to	Employees given these Access Levels
1	**Centre I**	All doors of the facility	Facility team (employees for server room door to be approved by Data center manager and Head of Facilities)
			Security team (employees for server room door to be approved by Data center manager and Head of Facilities)
2	**Centre II (except server rooms)**	All doors of the facility except Server room door	Facility team (employees for whom server room door is not approved by Data center manager or Head of Facilities)
			Security team (employees for whom server room door is not approved by Data center manager or Head of Facilities)
			Admin Head
			Center Head
3	**Tech I**	All doors of all general access areas (corridors, lobbies, common areas & Fire exit doors)	Tech Team members (employees for server room door to be approved by Data center manager)
		Telecom room door	
		HUB room door	
		Server room door	
		Operation floor doors (after taking approvals from all Process heads)	
		Support area doors	
4	**Tech II (excluding sever room door)**	All doors of all general access areas (corridors, lobbies, common areas & Fire exit doors)	Tech Team members (employees for whom server room door is not approved by Data center manager)
		Telecom room door	
		HUB room door	
		Operation floor doors (after taking approvals from all Process heads)	
		Support area doors	

5	**General**	Doors of all general areas (corridors, lobbies, common areas & Fire exit doors)	Support staff employees
			Employees - New / Bench/ Training
			Housekeeping staffs
6	**Process**	Doors of all general areas (corridors, lobbies, common areas & Fire exit doors)	Process employees
		Process floor doors	Client
		Support area doors	Security Guards posted at the process floor doors (1 card for each post)
			Trainers for process (subject to approval by Process head)
			HR SPOC for Process
7	**Out Station employees**	Doors of all general areas (corridors, lobbies, common areas & Fire exit doors)	Process employees
		Process floor doors	(access to process doors are subject to mail approval from process head)
		Support area doors	
8	**BMS room**	Doors of all general areas (corridors, lobbies, common areas & Fire exit doors)	CCTV/Access Control operator sitting in the BMS room
			Security Team
		BMS room door	If Facility team working in BMS room

12. Personnel Security

Adequate measures will be taken and implemented to ensure safety, security and wellbeing of employees and others while they are in the premises. Firstsource is committed to maintain a safe workplace environment and to deter and prevent any form of threat and or violence.

- Employees, service provider employees, visitors etc. will wear and display their respective ID Cards as specified in respective Geography SOP when within the Firstsource premises.
- All employees, service provider employees, visitors, clients, and others are to be informed of unauthorized / illegal items and material as specified in respective Geography SOP.
- Prohibited material including but not limited to: -
  - Illegal substances
  - Dangerous articles (knife/ weapons, acid etc.)
  - Alcoholic beverages

- Any other prohibited / unauthorized Firstsource materials

- Frisking will be conducted as per the law of the land and as specified in respective Geography SOP.

- Women Safety

  - Escorts where required will be provided for cabs carrying women employees if a woman employee is rostered for the first pick-up or the last drop during the period specified by the law of land.

- Random alcohol testing of drivers may be carried out by Firstsource.

13. Security of Information

Adequate controls including physical safeguards will be put in place to safeguard sensitive information and information systems including but not limited to: - Frisking metrics to be decided as specified in respective Geography SOP

- Employees are to be checked as per their respective designations. Exceptional cases will be considered after approval from the Security Head.

Designation	Frisking to be done	Baggage to be checked	Laptop to be checked
	Main Entrance	Main Entrance	Main Entrance
Agent	Yes	Yes	No
Team Leader	Yes	Yes	No
Asst. Manager	Yes	Yes	No
Manager & Sr. Manager	Yes	Yes	No
DGM	No	No	No
GM & Above	No	No	No
Client & Client Representative	Yes	Yes	Yes

- Frisking and checking of employees while entering the Operations floor is 100% and not negotiable (applicable where security guards are deployed at the process entrance, as per clients SLA).

- The authorisation list will be amended in case of any addition or deletion.

Authorization Control List For XXXX Center: XXX Process																	
Emp Code	Name	Function	Designation	Laptop	Smart Watch	Wallet / Purse	Camera Mobile	Non Camera Mobile	Pink Paper	White Paper	Note Book / Diary	Pen	Pencil	White Board Marker	Bag	Based out of process area	Frisking & Checking

- **Unauthorized Material and Escalation Matrix:** In case the following unauthorized materials are found being carried in and/ or out of the production floor by any person, without a proper authorisation from the Process Head or Head, Corporate Security, the following matrix will be followed to escalate the incident:

Description	Escalation Level 1	Escalation Level 2	Escalation Level 3	Escalation Level 4	Escalation Level 5

Laptop	Security Officer / Supervisor	Firstsource Security	Technology	Process head	CTO
Pen	Security Officer / Supervisor	Firstsource Security	Team Leader	Ops Manager	Process Head
Paper	Security Officer / Supervisor	Firstsource Security	Team Leader	Ops Manager	Process Head
Wallet	Security Officer / Supervisor	Firstsource Security	Team Leader	Ops Manager	Process Head
Bag	Security Officer / Supervisor	Firstsource Security	Team Leader	Ops Manager	Process Head
Narcotics / psychotropic substances	Security Officer / Supervisor	Firstsource Security	Line HR & Process Head	HR Head	Firstsource Security Head
Explosive devices	Security Officer / Supervisor	Firstsource Security	Firstsource Security Head	Process Head, HR Head	Police
Dangerous articles (knife/ dagger/ weapons, acid etc)	Security Officer / Supervisor	Firstsource Security	Line HR & Process Head	HR Head	Firstsource Security Head
Alcoholic beverages	Security Officer / Supervisor	Firstsource Security	Firstsource Security Head	Process Head	HR Head
Electronic medias like CD, Floppy, Pen drive, I-Pod, Digital diary, recording devices & mobile phones (with and without camera)	Security Officer / Supervisor	Firstsource Security	Technology	Process head	CTO
Any other unauthorized Firstsource material	Security Officer / Supervisor	Firstsource Security	Firstsource Security Head	Process Head	HR Head

14. Security of Operations

Adequate measures including physical safeguards will be implemented to safeguard business operations including the process floors in terms of access control, employee verification, asset protection and placing of E-Security systems. The following are prohibited: -

- Exchanging/ borrowing/ lending of access cards
- Tailgating

- Wherever mandated as per clients SLA, Security guards (male/ female) will be posted at the entry/ exit points to conduct frisking.

15. Security of Material / Asset

Adequate measures including physical and E-security safeguards will be put in place to safeguard Firstsource physical assets in terms of inventory control and loss prevention (waste, abuse, theft, and pilferage). Inward and or outward movement of the material would be permitted only on 'Gate Pass' basis. Gate pass process in detail is specified in respective Geography SOP.

- Fire Prevention and Protection / Suppression: Security team is responsible for fire safety protection program as they are already involved in emergency response, contingency planning and asset protection. Fire prevention education, awareness and training will be regularly conducted by the Security Team.
  - Participation in Fire Drills / Emergency Evacuation Drills is mandatory for all Firstsource employees. Process / Operations Head to provide exception approval if a particular Process is not participating in the drill.
  - Departments will nominate Fire Marshals for undergoing the fire safety training organized by the security team.

Fire Drills / Emergency Evacuation Drills will be conducted either quarterly, or twice a year at least, as specified in respective Geography SOP

16. Contingency Planning

Security team working in close coordination with the BCP Team will: -

- Secure and protect people.
- Secure the continuity of the core elements of the business – the infrastructure and the critical processes.

17. Investigations & Liaison

Security team is the in-house consultant on all crime prevention, workplace violence, enquiries, and investigative matters. The Security team is responsible for liaising with the police, other law enforcement agencies and the other investigative agencies. Security team will conduct routine and special investigations as assigned by the Firstsource management.

18. Executive Protection

As and when requisitioned, security team will take all necessary measures to ensure application of protective measures to reduce the risk to the executives and avoid and or control threats.

19. Security Education, Awareness and Training

- Security team will carry out 'security education, awareness and training' drives targeting all employees, regarding the security of the personnel, material, information, operations, and fire safety. These drives may be through briefings, emails, posters, newsletters, and online information.
- Annually, all employees will undertake the online security training and awareness session.

20. Occupational Health, Safety and Environment ("OHSE") Initiatives and Drives

The Security teams in each Firstsource centre will drive OHSE initiatives in their respective centres and will encourage participation and involvement of employees in such activities from time to time. OHSE policy in detail is specified in Global OHSE policy.

21. Standardization of the Guarding Services for Centers

Security cannot be template as each facility, location and the prevailing dynamic socio-economic factors pose a variety of challenges for security management. They affect and dictate security arrangements including deployment of the security guards. Appended are the recommended areas/ specific locations which ideally need to be manned / secured either physically or monitored through E-Security system and or have a judicious mix of both. Exceptions to this standard impacting the security posture will be signed off by the CAO.

	Standalone Facility		Multi Tenancy Facility	
Areas requiring deployment	**Number of Guards**	**Remarks**	**Number of Guards**	**Remarks**
Main Gate – Perimeter	2		NA	
Rear Gate – Perimeter	1	if not locked and covered by CCTV	NA	
Basement Parking	1		1	
DG Area	1	If not covered by CCTV or the prevailing local conditions dictate	1	If not covered by CCTV or the prevailing local conditions dictate
Main Entry / Reception Desk	1		1	
Frisking & Baggage Check at main entrance	2	Male and female guards- If independent floors with separate locker arrangements exists - same requirement per floor	2	Male and female guards- If independent floors with separate locker arrangements exists - same

					requirement per floor
Floor entrance	1	Per floor. If one floor has 02 separate entry for process, then there would be additional 01 guard		1	Per floor. If one floor has 02 separate entry for process, then there would be additional 01 guard
Material Gate	1			1	
Fire Exit Door	1	Per floor/ door - If not covered by CCTV and not connected with the ACS & Fire Panel		1	Per floor/ door - If not covered by CCTV and not connected with the ACS & Fire Panel
BMS Room	1	Per shift, 24 x 7 monitoring		1	Per shift 24 x 7 monitoring
Cab Escort		As per regulatory / statutory / HR policy			As per regulatory / statutory / HR policy
Process Floor Entry		Client SLA			Client SLA
Supervisors	1	Per shift		1	Per shift
Patrolling guard	1	Per shift per floor		1	Per shift per floor
Assignment Officer	1	In absence of Security manager		1	In absence of security manager
Total	**15**			**12**	

Change Control Information

Version	Changes Made	Revision Date
	NA	Nov 2022