AXACTOR

1000 Physical security policy

15.12.2022

Approved by the Axactor Board

Contents

1. Purpose

To describe the measures designed to deny unauthorized access to office facilities, equipment and resources, and to protect personnel and property from damage or harm.

The physical security policy shall also provide measures to safeguard employees from the threat of physical violence.

2. Target group

This policy, related procedures and supporting documents applies to all Directors of the Board, employees, including temporary employees, legal entities within the Axactor Group and where applicable to consultants and subcontractors, pursuant to the Axactor Corporate Governance policy.

3. Governing principles

3.1 Locations

Prior to signing new lease agreements, physical security arrangements for the potential rental property must be assessed.

All the premises shall comply with Axactor security arrangements. Costs related to close gap shall be included in the business case.

The responsible manager at each location shall on an on-going basis evaluate and manage security threats that premises under his/her responsibility are exposed to such as fire, flood, earthquake, explosion, smoke, theft, civil unrest and other forms of natural or man-made disaster. A yearly physical security risk analysis with proposal for actions shall be conducted.

3.2 Healthy, including and safe premises

Axactor's premises shall facilitate a safe and healthy workplace. Measure shall be made to prevent injuries in the workplace and danger to employees' health. The premises shall facilitate for employees with disabilities to enable a safe and including work environment.

All locations shall have the lowest possible energy consumption level and systems for time-regulated monitoring of ventilation, heating/cooling and lighting. Any reconstruction of current offices or relocation to new offices shall not lead to higher energy consumption.

3.3 Physical security perimeter

Physical security requirements that shall be in place to secure the physical perimeter:

- Perimeters of the building or site that contains the information facilities shall be secure. The roof, walls and flooring should be of solid construction to prevent the possibility of break-ins.
- All external doors shall be protected against unauthorized access, locked when unattended, and shall include access control mechanisms.
- All facilities shall be fitted with an up-to-date lightning protection system
- Risk based routines for visitor control.
- An intruder detection system should be installed and tested to cover all external doors and easily accessible windows.
- Unoccupied areas or server rooms should always be set up with market standard alarm system.

3.4 Securing offices, rooms and facilities

Key facilities should be rigged to avoid access by the public and configured to prevent confidential information or activities from being visible and audible from the outside.

Where possible, the rooms and facilities should give a minimum indication of their purpose.

Guidelines for eating and drinking in proximity to information processing facilities should be established. Smoking in Axactor offices and in proximity to information processing facilities shall be prohibited.

3.5 Delivering and loading areas

Access points such as delivery and loading areas should be restricted to identified and authorized personnel and if possible, isolated from information processing facilities to avoid unauthorized access.

Any incoming material should be inspected and examined for explosives, chemicals or other hazardous materials before being moved to another location.

3.6 Special protected areas

Critical office functions (e.g., room for servers or routers) and records (room for file lockers) must be locked and protected. Additional two-factor access authentication (or keys+PIN, card+PIN, etc.) is recommended. However, access to such facilities shall be restricted to authorized personnel only. Authorization may depend on time (normal office hour / not office hour).

Any access to a protected area shall be logged and recorded. Access rights to secure areas should be regularly reviewed and updated and revoked when necessary.

3.7 Debtor visits

Where and when debtors are allowed into the premisses, measures shall be in place to protect the employees at the relevant site. These routines shall ensure safeguards to prevent our employees from physical assaults from debtors. E.g., by making sure that employees are never left alone with the debtors, and that the facilities or rooms are arranged in a way that secures quick escape for the employee, possibly a panic button, and/or a physical barrier between the employee and the debtor.

3.8 Access Methods

3.8.1 Keys and badges

All offices must be locked with access control system based on individual employee identity card or individual access badge.

During normal office hours, when the office is manned, access to employees can be allowed by the access badge alone. Outside normal office hour, when the office may be unmanned, employee access shall be authenticated by two-factor authentication, for example by badge and PIN.

All offices must be protected by a key-lock system. Formal record of key distribution shall be maintained. A duplicate of the keys must be kept in the office safe or similar place, managed by HR department.

3.8.2 Visitors

Each country manager shall ensure that appropriate visitor control routines are in place where visitors are allowed into the premises. A risk-based approach shall be applied, and measures may vary depending on the type of visitors. Visitors shall never be allowed access unaccompanied to office facilities, and access should only be granted for specific and authorized purposes.

All employees shall be informed that they must notify immediately a manager if they encounter unescorted visitors.

3.8.3 Cleaning and maintenance workers

Cleaning and other maintenance work performed by external parties shall be done preferably within regular working hours or under the supervision of Axactor employees or security guards at production sites.

3.9 Workplaces

Employees shall follow the “Clean Desk Policy” and ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. This will reduce the risk of security breaches in the workplace and increase employee’s awareness about protecting sensitive information.

Main statements of the “Clean Desk Policy”:

1) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

2) Computers must be locked when workspace is unoccupied.

3) Computers must be shut completely down at the end of the workday, unless specifically required by the respective IT department on special occasions.

4) All documents, notepads and agendas must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the day.

5) File cabinets containing documents must be kept closed and locked when not in use, when not attended and at the end of the day. Keys mustn't be left unattended.

6) Printed documents should be immediately removed from the printer. It is mandatory to use printers with "PIN-code" function or "Follow-me" function where this functionality is technically possible. For locations where this is not supported by the current equipment, this shall be mandatory functionality when the equipment is replaced, unless an exception is granted by the COO.

7) Whiteboards should be erased after the meeting. In case of paper version, the used pages should be deleted after the meeting.

8) Storage devices such as DVD, portable hard disks or USB-drives must be secured in a locked drawer.

3.10 Transport of assets

Valuable assets such as company laptops or archives containing original documents must be properly safeguarded during transportation.

The company laptop must never be left unattended in public places and cannot be stored inside checked luggage when travelling by plane, only hand baggage can be used to store it.

3.11 Fire security and protection

The manager at each respective unit shall ensure that office facilities, all doors on the security perimeter and walls, are protected with fire detection systems and emergency fire extinguishing equipment at least complying with applicable regulations. A fire security assessment shall be carried out to ensure that adequate fire protection is in place. Employees shall be trained to handle fire situations and regular fire drills shall be undertaken for all business premises. Sufficient fire response measures shall be installed for the protection of valuable business assets that cannot be evacuated easily e.g., paper archives and server room equipment and due to a documented risk analysis.

3.12 Handling threats against employees

If an employee feels uncomfortable after a business discussion with a client, vendor or a debtor, they should report it to their manager. What is uncomfortable is a matter of individual judgement.

Threats or violent attacks against employees shall be reported locally to le respective HR department and to Group HR. As soon as possible the manager shall provide the necessary information available and discuss the matter with the relevant department. The HR department shall contact the person involved and agree upon further progress.

If needed in certain instances, legal expertise should be available. In those cases where Axactor advisors meet the debtor face to face and there is a threat of physical violence in addition to verbal abuse/threat, the advisor is recommended to withdraw from any situation which may cause any harassment.

If local legal expertise is recommended, management shall, in their cooperation with the legal expertise, decide upon appropriate action to be taken.

Submitting threats and conduct violent behaviour is punishable and shall as a general rule be reported to the local police to visualize that threats cannot be submitted without consequences. However, each and every case has to be considered carefully to see if this is the appropriate way of doing things (practice).

4. Local variations

Each unit – at company and/or country level – shall establish and maintain a local version of this policy, reflecting local arrangements, conditions and laws where necessary.

This policy is general and can be overridden by a stricter local policy which must be reviewed and approved by the COO at group level.

5. References

- ISO 27001/17799 Information Security Management System
- IT and Information Security policy
- Access control and administration procedure

Review log

Version	Date	Changed by	Comments
0.1	01.02.18	Oleg Khudiakov	Initial and changes according to Axactor Guideline for policies and procedures
0.2	01.03.18	Siv Farstad, Alexander Latenko, Ramon Calleja	Some things clarification
1.0	05.03.18	Endre Rangnes	CEO approval
1.1	24.11.18	Oleg Khudiakov	Changes according to Vibeke Ly and Maurizio Nannini comments
1.2	12.12.18	Vibeke Ly	Upgraded to policy and approved by the Board
1.3	12.12.19	Vibeke Ly	Approved by the Board
1.4	24.02.20	Eva Rodríguez	New content added, reorganization and review with comments
1.5	15.06.20	Vibeke Ly	Board approval
1.6	15.12.21	Vibeke Ly and Arnt-André Dullum	Board approval; various minor adaptions
2.0	15.12.22	COO / Chief of Staff	Minor updates.