Reviewed by: Antti Kutila 15/12/2018
Signature/Date

Approved by: Joseph Nazareth 15/12/2018
Head of Group HSEQ Signature/Date

Table of Contents

1.1 Objective

The objective of this SOP for physical security of ISS premises is to standardise and develop security procedures and operating methods to protect ISS assets including:

- Personnel;
- Information (ISS and Customer);
- Premises (property) and
- Reputation.

1.2 Application

This SOP applies to ISS premises in operational countries and is mandatory for countries based on:

- Percentage of Group revenues and
- Considered high risk*.

* As determined by a third party such as Zurich Risk Room.

1.3 Responsibility

Country Management	Responsible for implementation of this SOP.
Security Responsible	Responsible for security in the country with competencies in security.
Premises (Property) responsible	Responsible that security arrangements are taken into account and implemented for the premises in accordance with the instructions from the Security Responsible.
Employees	All employees have the responsibility to act according to security and safety guidelines and the training they have received, be alert about their surroundings and to reaffirm the necessary focus on the safety of our colleagues, our customers and our premises.

1.4 Definitions and Abbreviations

GDPR	EU General Data Protection Regulation.
High risk sites	Sites located in countries rated as high risk based on the risks due to: • Armed conflict; • Crime; • Terrorism. A list of countries is maintained by Group Risk Management.
Premise	All sites including ISS owned and leased premises, buildings, offices, data centres, warehouses, etc. where ISS manages, supports and manages operations.
Risk	The possibility of loss resulting from a threat, security incident or event.
Risk Assessment	The Process of assessing security-related risks from internal and external threats to personnel, information, premises and reputation.
Security Incident	A security-related event such as theft or assault against employee.

Security Vulnerability	An exploitable security weakness or deficiency at a facility, entity, venue or of a person.
Threat	An intent of damage or injury; an indication of something impending.

1.5 Requirements

Security procedures related to ISS's premises shall consider protection of personnel, information, assets and reputation.

1.5.1 General

As part of the safety and security of ISS premises (and as a part of development), it is necessary to identify at least the following requirements:

- ISS internal guidelines (security, safety, risk management, business continuity);
- Requirements from customers;
- Requirements from insurance companies;
- Local legislation (e.g. fire safety regulations);
- GDPR.

1.5.2 Security Risk Assessments

Risk Assessments shall be taken for each premise and must be documented and reviewed at least every 12 months.

The security Risk Assessments shall consider:

- Harm to people – safety and security; including employees, trainees, customers, visitors, guests, vendors, tenants, contract employees;
- Intentional damage to premises resulting from criminal activities causing physical damage to premises;
- Unauthorised access: The risk of financial/non-financial loss/information leak/loss, to the business leading to interruption or reputational damage due to inappropriate/unauthorised access to secure areas in the building including data centres. This does not include unauthorised access to IT systems (by internal staff or through cyber-attack) leading to breach of information assets;
- Theft or intentional damage to assets: The risk of financial/non-financial loss to ISS caused by theft or damage to assets (e.g. cash, keys, material kept in safe keeping). There are 3 associated risks:
    - Theft of assets by external party;
    - Theft of assets by member of staff;
    - Intentional damage to assets, including arson.

1.5.3 Premise Security Plan

Purpose	The purpose of a Premise Security Plan is to describe and create security-related systems, arrangements and operating methods. The approach will achieve consistent, thoughtful and corresponding response for needs.

Development of a Premise Security Plan

A site security plan shall be developed based on quantitative and qualitative criteria.

Examples of Quantitative criteria:

Harm to people	• Loss of life of an employee, customer, or member of the public • Critical injury to an employee, customer or member of the public • Kidnapping, hostage taking, siege • Extortion and or criminal intimidation • Discharge of a firearm or use of any other weapon with the intent to harm people
Unauthorised access to premises	• Has caused major business disruption to a Mission Critical premises or significant disruption to any Critical premises resulting in severe customer or business inconvenience
Theft or intentional damage	• Burglary • Arson • Attempts to force an employee to handover cash or information?

Qualitative criteria: This is about the probability of a risk occurring and its impact on ISS (e.g., financial, reputational, etc.).

Premise Security Plan contents

A Premise Security Plan should contain the following elements:

1. Structural security solutions	• Outdoor areas (fences, gates, signage) • Walls • Doors, Windows and openings • Locking • Safes (and strongboxes)

2. Technical Security and safety solutions	• Lights (outdoor, emergency, guidance) • Access Control • Intrusion Detection Systems • Fire alarm system
3. Security Practices and security culture	• Security Guidelines • Security Training (for personnel) • Office policies • ID-cards • Visitor management (visitor badge, escorting, meeting facilities) • Notifications (security and safety notifications from employees)
4. Security Procedures and controls	• Reception • Guarding • Access hours and levels of access • Parking • Key management • Emergency actions • Security manuals and guidelines for security personnel • Site safety plan • Raising the level of security • Maintenance and testing of security systems

1.5.4 Security searches

Security searches can be termed as routine, snap or planned and may be conducted in accordance with customer requirements and must always be conducted according to local legislation. A defined process must be in place to identify personnel authorised to undertake security searches, ensuring they are competent and trained in approved searching techniques. Security searches must only be carried out by personnel authorised as part of this process. All personnel responsible for carrying out searches must be made aware of the scope of their powers in respect of local legislation and guidance.

All pre-planned and routine security searches on personnel, facilities and vehicles must have prior written authorisation from the Security responsible

and only after engagement with local P&C and local Legal. For non-planned searches, clear reporting and escalating procedures must be in place.

Clear procedures must be established for escalating cases where the search team have reasonable grounds to believe that a crime has been or is being committed.

All searches must be recorded, independently witnessed and include as a minimum:

- Date, time and location of the search/area searches;
- Full name of person conducting the search;
- Purpose of the search;
- Communication of the purpose of the search to the individual being searched and their response (if appropriate);
- Reason for decline (if appropriate) and details of escalation where appropriate;
- Search results and follow up actions;
- For people searches, the full name of the individual being searched must be recorded;
- Name of an independent witness who has not conducted any element of the search.

1.5.5 Security incident management

All security incidents shall be reported in the incident management module in the HSEQ@ISS-IT system, VelocityEHS.

Incidents shall be investigated to determine the root causes and appropriate corrective and preventative actions determined to address the identified root causes.

1.6 References

- ISS Security Policy
- ISS IT Security Policy
- ISS Information Security Policy

1.7 Assurance

Applicable countries shall have a security risk assessment that is reviewed every year and a Premise Security Plan as per this SOP. This shall be sent to Group HSEQ and CR.

APPENDIX A: BUILDING SECURITY CHECKLIST

1. Are all external doors and ground floor windows secured when the building is closed for business?
2. Are there durable wall structures?
3. Are there security related signs (guarding, CCTV)?
4. Are there no burning materials available in the immediate vicinity (consider the trash cans)?
5. Are doors, windows and openings protected?
6. Is the securing (locking) of the premises address the need?
7. Is there an intrusion detection system on the property?
8. Is there an access control system on the property?
9. Is there a CCTV system in the property?
10. Are there security layers (layers by purpose; see Appendix B for guidance)?
11. Do lifts/elevators allowing public access open into an area segregated from controlled space.
12. Is all IT equipment determined by the Security Risk Assessment to be critical to the business secured to prevent unauthorised access or theft?
13. Where IT equipment rooms exist, are all critical IT equipment stored in a secure environment?
14. Are safes and strongboxes available (especially for keys)?
15. Where access to keys needs to be strictly managed and controlled, is there a documented key management, access and control process in place?
16. Are any keys removed from premises kept on unlabelled, untagged key rings?
17. Are lock combinations only known by authorised individuals?
18. Is a register of the lock combination holders and the type of access maintained? All combination changes must be recorded in this register alongside the reason for the combination change.
19. Is the combination of each lock changed at intervals and documented?
20. Are employees wearing ISS ID-badges (picture)?
21. Is there a clean table policy?
22. Is there clean screen policy (computer locked when an employee leaves their desk)?
23. Is the protection, storage and disposal of restricted and confidential material (e.g. confidential waste bins, shredders) conducted in accordance with procedures?
24. In all ISS buildings defined under this procedure, where visitors enter a controlled space, are all visitors being signed / booked in.? Where a pass is issued, does it clearly identify them as a visitor?

25. Do visitors wear their pass always whilst on the premises?
26. Are visitors allowed unescorted access to restricted Security areas?
27. Are security guidelines available?
28. Is there security training for employees?
29. Is there an Emergency Response Plan for the property?
30. Are fire extinguishers available (in working order)?
31. Are emergency exits free (no obstacles)?
32. Are emergency signs displayed (emergency exits, fire extinguishers, first aid, defibrillator)?

APPENDIX B: PROTECTIVE LAYERS

Outer protective layer or perimeter; is the outermost point at which physical security measures are used to deter, delay and respond against illegitimate and unauthorized actions.

Middle protective layer; exterior of building.

Inner protective layer(s); usually several inner layers are established; their placement is designated to address an intruder who penetrates outer and middle protective layers.