INSTRO PRECISION LIMITED

SECURITY POLICY

A vigilant workforce is a secure workforce

Instro Precision is committed to managing security risks related to the conduct of its business. It does this by providing the necessary analysis, assessment, prevention, assurance and response activities required to minimise loss, damage and compromise of assets.

Instro Precision requires information management and technology systems and solutions that are secure, value for money and interoperable to support the flow of information across the organisation. Personal behaviour is fundamental to good security and it is each employee's personal responsibility to work in accordance with the Instro Precisions Security Policy and relevant security standards to preserve a secure working information and to prevent loss, damage or compromise of assets.

All employees have the personal responsibility to familiarise themselves and comply with their local Security policies and procedures which includes but is not limited to :

- Integrated Management System Policy
- Security Handbook
- Configuration & Change Management
- Security & Configuration Management Policy
- Information Sharing Handling & Transport Policy
- Visitor Access Procedure
- Access Control Policy
- Password Policy
- Acceptable Use Policy
- Mobile Device Policy
- Incident Management Policy
- User Security Obligations & Disciplinary Procedure
- Asset Management Policy
- Business Continuity & Crisis Management Plan

applicable national laws, regulations and contractual obligations including but not limited to:

- ISO 27001 Information Security Management
- United Kingdom Security Vetting (UKSV)
- Facility Security Clearance (FSC) Policy and Guidance for UK Defence Contractors and MOD Contracting Authorities
- JSP440 Annex S – Memorandum of Security for UK MOD Contractors
- Government Functional Standard 007 (GovS 007: Security)
- International Visits Control Office (IVCO) Guidance Notes for MOD List X Contractors
- Official Secrets Act (OSA)
- The Data Protection Act (UK's implementation of the EU's General Data Protection Regulation (GDPR))
- The Computer Misuse Act
- Freedom of Information Act
- General Data Protection Regulation (GDPR)

Personnel (Staff)

All employees (employed and contracted) are required to meet Baseline Personnel Security (BPSS), as a minimum requirement prior to commencing employment. BPSS allows access to UK OFFICIAL assets and occasional access to UK SECRET assets.

Additionally, employees who regularly work with or have 'need-to-know' access to UK MOD Identifiable Information or Assets with a classification of OFFICIAL-SENSITIVE will be subject to the additional Security Check (SC) requirement.

Employees who are verified as holding SC clearance can be given 'need-to-know' access to any Information or Assets with a classification of SECRET.

Employees with 'Need-to-know' access to Information or Assets with a classification of TOP SECRET must hold Developed Vetting (DV) clearance and must comply with both the internal Information Security Management System (ISMS) and Company Security Instructions (CSI)1 requirements.

Employees are to be given Security training and awareness upon joining the company and refresher training on at least a three year basis.

Employees with specific roles and responsibilities for security must be suitably qualified and experienced for such roles.

Employees who work with UK MOD Identifiable Information or Assets are required to sign the Official Secrets Act when they both join and leave the company.

Employees are required to conform with the Elbit Systems Ltd Corporate Social Media Policy.

They must report security concerns or breaches of security promptly in accordance with local Security policies / instructions and dispose of assets in accordance with applicable security, contractual and regulatory requirements.

Personnel (Visitors)

Visitors to any site must comply with both internal Information Security Management System (ISMS) and International Visits Control Office (IVCO) requirements (where the visit is to a site with a Facility Security Clearance (FSC)).

Instro Precision Visitor and Access Procedure provides guidance on the visitor process, it will include the requirement to ensure that all visitors are always distinguishable from employees e.g., using a lanyard or badge.

Specific IVCO requirements for FSC sites include the following:

- Visitors from Countries who are part of the Multi-national Industrial Security Working Group (MISWG), which includes Israel, are not required to submit a Request for Visit (RFV) if the nature of the visit does not exceed OFFICIAL-SENSITIVE.

- If the Visit requires access to Information or Assets above OFFICIAL-SENSITVE an RFV will need to be submitted by the Visitor and approved prior to the visit taking place.

- If a Visitor is from a Country that is not part of the MISWG an RFV will need to be submitted by the Visitor and approved prior to the visit taking place. Without an approved RFV they may be granted access to the Un-cleared Visitor Area (UVA) only and any discussions or access to Information or Assets must remain unclassified (note this does not apply to Chinese or Russian nationals who are required to submit an RFV for all visits).

Physical

Physical security includes measures to protect Instro's physical assets such as hardware, infrastructure, buildings, equipment and servers.

A Need-to-Know principle will be adopted for access to all information irrespective of the position, seniority or clearance held by an individual within the organisation.

All site key holders must have a valid Security Clearance (SC) or Personnel Security Clearance (PSC) equivalency in place if the site holds an FSC.

Only employees are to be permanently issued with Access Control passes for external and internal doors.

Visitors whose Security Clearance, 'need-to-know' and IVCO compliant status (as required for FSC sites) has been confirmed can be granted a temporary Access Control passes to the office areas for use during the working day. They must be returned at the end of each working day to reception and should the need arise be re-issued the following working day. Further they will only be granted access to the areas based on the Need-to-Know confirmation

All other Visitors can be granted a temporary Access Control pass to the Uncleared Visitor Area(s) only.

The master Key for all internal doors (except those to FSC Secure Areas) will be kept in a separate key safe and only accessible by the site key holders.

The Key, Access Control Fob or Access Code for any FSC Secure Areas where classified SECRET Information or Assets will be handled or stored will be kept in a separate key safe (BASE Protection Level container with a CLASS 3 Lock) and only accessible by the Board Security Contact, Security Controller, Deputy Security Controller and any additional Staff who have a confirmed Need-to-Know requirement.

In addition to Health and Safety practice evacuations, FSC sites must have up-to-date plans in place and rehearse evacuation, terror incident and site avoidance procedures at least annually.

No Personal Electronic Devices (PEDS) are to be taken into any FSC Secure Areas where classified SECRET Information or Assets will be handled or stored, mobile phone lockers will be provided to store devices securely elsewhere.

Each site will conduct and document physical security risk assessments in line with the UK's Centre for Protection of National Infrastructure (CPNI) Operational Requirements. Physical security controls (including but not limited to CCTV, alarms, automated access controls systems, doors, locks and keys) will be implemented in line with identified security risks.

Security guarding services provided by suitable accredited and vetted personnel will be provided at the site, they will conduct security patrols, monitoring of CCTV, responding to alarms and ensure a robust security culture exists at the site.

Instro shall establish and sustain regular links with local Police and the National Counter Terrorism Security Office (NaCTSO) and local Counter Terrorism Security Advisers (CTSA). NaCTSO is a Police unit that supports the 'protect and prepare' strands of the government's counter terrorism strategy. Regular Police site visits will be requested followed by independent penetration tests (physical and electronic).

Information

Information includes all of an organization's information assets, both physical and digital, as well as the processes and procedures used to manage them. This includes but is not limited to:

- Hardware: All hardware, such as desktops, laptops, smartphones, and tablets
- Software: All software
- Devices: All devices, such as desktops, laptops, smartphones, and tablets
- Offices: All offices
- People: All people who have access to any or all of the above

A Need-to-Know principle will be adopted for access to all information irrespective of the position, seniority or clearance held by an individual within the organisation.

An Information Security Management System (ISMS) will be implemented based on ISO 27001 to ensure that business financial information, intellectual property, employee details and information entrusted by third parties is kept secure.

All IT Systems processing MoD Identifiable Information will be approved for use (accredited) in accordance with MoD Cyber Defence and Risk (CyDR) Policy.

For FSC sites a Company Security Instructions (CSI) guidance document will be provided to all employees to ensure they understand their personal responsibility whilst handling and protecting information or assets in line with the Government Security Classification scheme (GSC).

A Clear Desk and Clear Screen Policy is enforced.

Approved shredders or a shredding service will be put in place to enable appropriate destruction of paper based information assets.

Only company owned and controlled devices (Computers, Laptops, Tablets, Phones, and Removable Media etc.) are to be connected (physically or logically) to the IT Network.

Web access to the Email System and SharePoint Site is permitted subject to it not being possible to download any attachments or documents to non-company owned and controlled devices.

Site Closures

Preventative and response measures for site closures are the responsibility of the Managing Director or Operations Director, these should be considered as part of a Business Continuity Plan.

As guidance, a site may be closed when there is a:

- Failure of a critical system/s preventing the site from being used
- Risk of harm to employees or visitors
- Risk of damage to employees or visitor's property
- When advised by the police or any other security agency to do so

The Managing Director has the full authority to close site (Instro do not require permission from Elbit Systems Ltd in Israel, as the legal responsibility must reside in the UK).

Media and Public Relations

A media response may be appropriate in certain circumstances, if action is required in a Security context then this shall be decided by the Managing Director in consultation with ESUK's Head of Security, Media and PR team.

Business Continuity

Instro Precision shall produce and implement a Business Continuity and Disaster Recovery Plan.

These commitments apply to all employees of Instro Precision, our suppliers and subcontractors (where appropriate). Additionally, we undertake to use our best endeavors to ensure that our business partners also abide by this policy.

Senior management is responsible for ensuring compliance with this policy, including but not limited to the establishment of programmes and compliance, however is the responsibility of all of us, at every level within our organisation.

The Managing Director of Instro Precision is ultimately responsible for this policy and the company's information security performance and is assisted by the management team, which oversees the implementation of all integrated management system procedures and programs within Instro Precision.

Dagan Yogev
Managing Director
31st July 2024

This version is created in accordance with Instro Precision Limited's Statement of Applicability – Issue 1 and cancels and replaces all previous versions.