ISM CW2

Framework of Security Policies

Student ID: 2136685

Table of Contents

Table of Figures

Table of Tables

Framework of Security Policies

Policy Name	Policy Overview	Policy Requirements	Policy Standards or Laws
Access Control Policy	The policy applies to all contractual relationships of the company, including the supervisors, employees, all visitors, and third parties who may require access to the company's assets, from unclassified assets to top secret assets.	1. Physical access to locations on site must be accessed only by personnel with the appropriate security clearance access given by the Security Controller. 2. Access to information assets must be given on a 'need to know' basis and approved by the Security Controller. 3. Officials with a statutory right of entry, such as statutory inspectors, can access assets classified as SECRET and above only if they cannot perform their duty without access to such assets. 4. All the company's systems are surveilled for monitoring and auditing purposes. 5. Only employees selected by the Security Controller may work on CLASSIFIED information at home, with some being allowed to work on SECRET material if they provide an approved security container.	Security Requirements for List X Contractors
Data Protection Policy	This policy outlines the way all data is processed, stored, transferred, and disposed according to the UK data laws.	This policy follows the General Data Protection Regulation of the United Kingdom which outlines how all data must be collected, stored and destroyed: 1. All data must be lawfully and transparently collected and used and in a way that is fair. 2. All data collection must have a clear purpose for processing and the reasoning must be documented and specified. 3. All data collected must be adequate, relevant, and limited to the purpose of processing. 4. All data must not be incorrect or misleading and it must be kept updated for its purposes. 5. All data must not be kept for longer than necessary. 6. All data must be processed in a way that ensures that unauthorised or unlawful access is prohibited to protect against accidental loss, damage or destruction.	UK GDPR, Security Requirements for List X Contractors
Physical Security Policy	This policy depicts the minimum requirements for protecting the company's physical assets, including access control, surveillance and physical topology.	The company has a List X facility where classified material is held and where such work and conversations are being held. The Un-cleared Visitor Areas (UVAs) must be kept physically separate from the List X facility through access controls or being held in a separate building, to ensure that no classified information is being accidentally viewed and that no classified conversations are being overheard. Access to buildings must be done through security badges, either by using them on access points or by showing them to the security guards. These access points should be guarded by CCTV.	Security Requirements for List X Contractors
Incident Response and Business Continuity Policy	This policy establishes the procedures and requirements for a response in the event of an incident to ensure the continuity of the business, including backup and recovery, and disaster recovery testing	Any security incident involving official information must be reported to the appropriate management channels. Any security incident involving classified information must be reported to the Contracting Authority. Any security incident involving Ministry of Defence (MOD) owned, processed or generated information must be reported to the MOD Defence Industry Warning, Advice and Reporting Point (WARP). The security incidents must be assessed, and the knowledge gained from them must be used to reduce the likelihood of such events occurring in the future. To ensure business continuity, the team must monitor the disruption and the organisation's response to it. The team must ensure that the delivery of the product is still in the timeframe projected, this might require actions such as recovering from backups.	Security Requirements for List X Contractors, ISO 22301:2019
Security Awareness and Training Policy	This policy outlines the requirements for educating and training the employees for security best practices and how to recognise phishing attacks, social engineering and how to properly report an incident.	The company must ensure that the employees are well trained in the event of a fraudulent attack, such as social engineering attacks. Employees must know that any company official will not contact them to ask for credentials. Employees must be made aware of the techniques used in such attacks and the standard procedures to response to these attacks. Employees must know who to contact in case of an attack, especially in the case of CLASSIFIED information being compromised. Employees must keep CLASSIFIED material locked away, in an appropriate container, when not being worked on.	NIST SP 800-53, REV. 5, Security Requirements for List X

Table 1 - Framework of Policies (gov.uk, 2014; iCIMS, 2018; ICO, 2022; ISO, 2019; NIST, 2020; University of Warwick, 2020a; University of Warwick, 2020b)

Security Controls

Physical Security

Physical security entails a range of controls, including preventative, detective and corrective controls.

Firstly, ensuring that the List X building is separate to the Un-cleared Visitors Areas (UVAs), to ensure that classified information is not accidentally left for visitors to access, or for them to overhear classified conversations, as per the Government's Security Requirements for List X Contractors. These buildings can be further split into unrestricted, controlled, limited and exclusion areas to further tighten access, as seen in Figure 1 (gov.uk, 2014; Stein, 2023).

The building should ensure that work can continue even during a power problem, including cuts and surges. Therefore, the company must have Uninterruptible Power Supplies (UPSs) and emergency generators, so that workers can at least save their work.

Preventative controls, such as fencing the company building and placing no trespassing signs around the perimeter, to deter people from unauthorised access to the premises, and to funnel people towards the security-controlled entrance. Barriers can also be placed around the fence to point to the correct entrance, or to block certain corridors that lead to classified spaces.

Guards must patrol the premises, to apprehend unauthorised visitors from access to classified places, accidental or intentional. Along with guards, detective methods such as CCTV cameras will be around the perimeter, attached to a real-time surveillance system to be able to always monitor the premises. Good lighting is necessary for the CCTV cameras to capture accurate details about the person, so lighting is crucial to be placed around the perimeter, including the parking spaces.

High-risk areas, such as the main entrances and entrances in between areas should have manned security points fitted with security measures such as metal detectors and X-Ray scanners for bags, to prevent people from bringing unauthorised items into the building, or to detect surveillance devices such as microphones attached to visitors.

Where un-cleared visitors are cleared and allowed access to the List X building by the Security Controller, they must be escorted and surveilled by security guards at all times. Visitors only have 'need to know' access, therefore the security guards must not allow the visitor to trail away from their given access.

Where there are no manned security points, the doors must be always locked, and only available to the personnel that has the appropriate clearance. For example, server rooms must only be accessible by network engineers and above, or the power supply room must only be available to electrical engineers and above, whereas lunchrooms and common rooms can be left unlocked.

If visitors can bypass these controls, some rooms such as the power supply room and the server room can be made human-incompatible. These rooms can be without windows, dimly lit, cramped and even have low oxygen, to deter humans from accessing them, or to limit the time they have access to these rooms.

Motion detectors, silent alarms and loud alarms must be implemented to detect unwanted access to classified zones. The motion detectors should trigger the silent alarms and contact the appropriate authorities, whereas the loud alarms should trigger if the threat actor gets too close to critical information, causing doors to lock and for the threat actor to be locked in a room where the authorities can quickly pinpoint.

Preventative and corrective methods against disasters, such as electrical fires, flooding, rapid change in climate, must be in place, such as smoke detectors, heat detectors, a ventilation system with dust filters and temperature regulation, and automatic fire suppression equipment such as gaseous fire suppression for server rooms and power supply rooms, and water sprinklers for rooms without critical electronic infrastructure, such as the common room. No smoking signs should be placed around the building as well, as the law dictates (Government Digital Service, 2012).

Access Control

Personnel must only be allowed the necessary access for them to conduct their work. Preventative methods should be put in place, such as a hierarchy of roles, to ensure that clearance is segmented and granular for parts of the List X building and the UVAs. These can be implemented by having access points use biometrics, or smart cards, or both for two-factor authentication. The access points can store logs of entries and exits to keep track of personnel going in and out of areas.

The employees should be given network credentials that they can use to log into company computers and company laptops. These computers should be controlled and restricted with the enterprise mode of Windows 10 and physical network filters, to ensure that the employees can’t install and run any application, such as viruses. The company should restrict the use of removable media, to ensure that a threat actor doesn’t inject viruses into computers left unlocked and that employees don’t plug a found USB into the company computer.

For networks, de-militarized zones and firewalls should be in place to ensure only the necessary traffic travels through the network, such as allowing traffic to flow to the website servers and the email server. These firewalls should hold logs of packets, for network engineers to analyse for potential threats in advance. Wireless Access Points should be secured with WPA3 encryption to ensure that threat actors cannot sniff packets and gain access to personnel information. VPNs should be used for remote workers with static IPs for them to be able to use the local network resources. Static IPs can recognise intruders, as if a user is connecting from a different IP, their account should get blocked.

Security Awareness and Training

People are usually called the weakest link in security; therefore, a company must do everything they can to educate them to achieve the best security.

To prevent threat actors from infiltrating the company, recruiters should make a judgment of character based on interviews, background checks, certifications and evaluations. Recruiters should also make sure that the approved applicants sign non-disclosure agreements so that nothing about the classified work is discussed.

Management should enforce mandatory security training and verbal reinforcement of good security practices, including attacks such as phishing and social engineering, and methods to protect RFID cards and NFC cards with Faraday pouches or RFID blocking plates in wallets.

Deployment Plan

To implement the above policy completely, the company must ensure that the framework of policies is well communicated to all employees and afterwards, the policy should be integrated into the employees’ security training. The policy should be enforced as soon as mandatory training ends, and the company must monitor the compliance to ensure that the policy’s guidelines are followed. If employees are not complying with the policy, the importance of following it must be reiterated, and perhaps punishments can be dealt, such as having to do another mandatory training course.

References

gov.uk (2014). *Security Requirements for List X Contractors*. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/367514/Security_Requirements_for_List_X_Contractors.pdf [Accessed 20 Mar. 2023].

Government Digital Service (2012). *Smoking at work: the law*. [online] GOV.UK. Available at: https://www.gov.uk/smoking-at-work-the-law [Accessed 21 Mar. 2023].

iCIMS (2018). *Information Security INCIDENT RESPONSE POLICY & PROCEDURES Policy Document*. [online] Available at: https://www.icims.com/wp-content/uploads/2020/09/Incident_Response_Policy_and_Procedures_2020.pdf [Accessed 20 Mar. 2023].

ICO (2019a). *Principle (a): Lawfulness, fairness and transparency*. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ [Accessed 20 Mar. 2023].

ICO (2019b). *Principle (b): Purpose limitation*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ [Accessed 20 Mar. 2023].

ICO (2019c). *Principle (c): Data minimisation*. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ [Accessed 20 Mar. 2023].

ICO (2019d). *Principle (d): Accuracy*. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/ [Accessed 20 Mar. 2023].

ICO (2019e). *Principle (e): Storage limitation*. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ [Accessed 20 Mar. 2023].

ICO (2019f). *Security*. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ [Accessed 20 Mar. 2023].

ICO (2022). *Guide to the General Data Protection Regulation (GDPR)*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed 20 Mar. 2023].

ISO (2019). *ISO 22301*. [online] ISO. Available at: https://www.iso.org/standard/75106.html [Accessed 20 Mar. 2023].

NIST (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controls for Information Systems and Organizations*, [online] 5(5). Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Accessed 20 Mar. 2023].

Stein, B. (2023). *New NIST Publication Recommends Best Fits Between Federal 'Locks' and 'Keys'*. [online] NIST. Available at: https://www.nist.gov/news-events/news/2008/04/new-nist-publication-recommends-best-fits-between-federal-locks-and-keys [Accessed 21 Mar. 2023].

University of Warwick (2020a). *IG02: Data Protection Policy*. [online] warwick.ac.uk. Available at: https://warwick.ac.uk/services/sim/policies/information-governance/ig02 [Accessed 20 Mar. 2023].

University of Warwick (2020b). *IS02: Access Control Policy*. [online] warwick.ac.uk. Available at: https://warwick.ac.uk/services/sim/policies/information-security/is02/.

Appendix

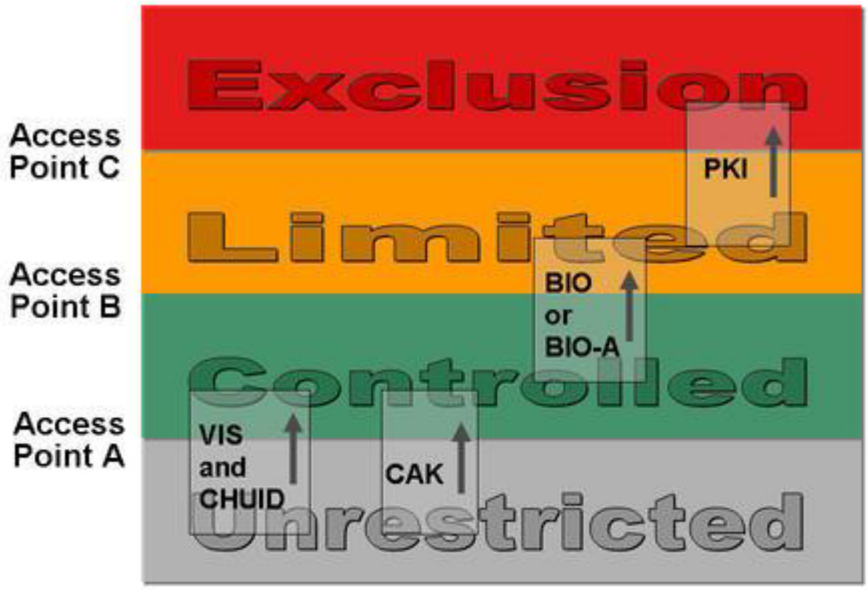

Figure 1 - Four Areas of Security in a Facility (Stein, 2023).