instrumentel
MEASURING SUCCESS

Cyber Security Policy

Purpose

This document is part of the Instrumentel suite of documents related to IT infrastructure, internet access and Cyber security design. The purpose of this document is to emphasise the importance of cyber security, not only within the work place but also in the design of all systems created and utilised by the company.

Scope

Who is covered by the policy?

This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, , wherever located (collectively referred to as employees in this policy).

This policy covers:

- Risk assessment management
- Cyber security within the design
- Protecting against attacks
- General guidance (applicable to all systems)
- Handling of any threats

Overview

Cyber attack poses a growing threat to the security and therefore the safety of infrastructure in Great Britain (and other nations with whom we may work). Expert opinion and research suggest that cyber systems are likely to contain vulnerabilities through insufficient protection. We will build in cyber security to all aspects of the business to ensure that our systems are designed and maintained with cyber safety in mind from the foundations up. This approach adopts a protection against cyber attack in line with the As Low As Reasonably Practicable (ALARP) principle as it relates specifically to efforts made towards the mitigation of threats and vulnerabilities.

Threats

The movement of the world towards a collaborative open-platform system wherein sensors can feature on the Internet of Things (IoT) leads to increased vulnerability to cyber attacks. Threats to these systems can come in a number of forms including:

- Remotely, via the internet or through unsecured Telcom networks
- Direct connection (i.e. through a communication port such as USB or Ethernet)
- Direct infiltration

These vulnerabilities can be through:

- Policy and procedure
- Architecture and design
- Configuration and maintenance
- Physical intrusion
- Software development
- Communication and network
- Lack of training and awareness

The impacts of these threats can result in:

- Threats to safety
- Disruption to service
- Economic loss
- Reputational damage
- Loss of commercial or sensitive information
- Criminal damage

To combat all of these our policy is to design systems that can be resilient to such attacks. These measures take into account the likelihood and impact of both deliberate and non-deliberate attacks in the first instance. These steps should also mitigate against the consequences of a successful attack – i.e what steps should be taken should an attack prove successful.

Risk assessment management

In line with other management systems (including ISO9001) risk and risk management will be built into to all products and design. Risk assessments (RA) are to be carried out to ascertain the probability and impact of any breach in security at both a physical and logical level. Any mitigation steps that are required to bring the risk into acceptable ranges should be applied then the RA repeated to show the mitigated level.

The management of the risk will be considered and reviewed during the product's full lifecycle including design, decommissioning and disposal.

Any third-party systems will be scrutinised for potential security weakness at a system level, applying the same level of RA.

Review

As risks will inherently change over time, risks to systems will be reviewed periodically (1 yr minimum) to ensure risks are kept to an acceptable level.

Cyber security within the design

Security requirements should be designed in from the start of the design process. This will indicate any compliance that will be required both at a customer and supplier level. Mechanisms are to be instigated to ensure that the security systems are upgraded, updated and maintained for the duration of their lifecycle. Any system disposal should be done so securely to ensure that data is effectively destroyed.

Design and development

Protective measures will be put in place on any system interface to ensure there is no unauthorised access, these methods can include (but are not limited to) user name and password authentication, logical keys, Access Control List (ACL), encryption and firewalling.

Installation

As a priority, the installation of a new or upgraded system should not compromise the security that has already been put in place. In order to achieve this, boundaries will be set between interfaces with other systems and wherever possible ‘air gaps’ should be implemented to ensure no soft connection is achievable. No changes should be made without completing a risk analysis to understand the impact they may make from a security perspective.

Maintenance

Systems are to be maintained throughout their full lifecycle to ensure that they optimally function. Any new developments in malware or other threats should be considered and if required patches applied to mitigate the threat. Where possible systems should be monitored and analysed for abnormal functionality or any indications of suspicious behaviour.

Decommissioning and disposal

During the decommissioning of any system it should be ensured that no hostile third party can acquire the data or programs.

Protecting against attacks

Application of good maintenance procedures in combination with system monitoring will allow the ability to protect against attacks. Any potential threat identified during the life cycle of the system should be dealt with on a risk basis (as outlined within the RA). Where patching is required, consideration should be given to other vulnerabilities that could be affected with the system to ensure that they are within acceptable levels.

Firewalls will be setup in accordance with the manufacturer’s instructions whilst being maintained, monitored and patched within it’s standard operating procedure. Subscriptions to any security mailing lists should be obtained to receive up to date information on newly discovered vulnerabilities. Any non-supported vendor equipment should be risk assessed for potential threats as support of these will still be required by Instrumentel.

General guidance

Capability and competence

All employees are to have general awareness of cyber security as delivered through the Unipart Way digital interface. All employees directly responsible for the design of cyber secure systems are to regularly review updated regulatory documents and receive training to ensure they are updated to keep up with the rapidly changing risks.

Behaviour and/or activities that threaten the integrity of the company’s computer networks or systems are expressly prohibited. Such behaviour and/or activities include but are not limited to:

- Interference/disruption of systems, networks or related services, including but not limited to the propagation of computer ‘worms,’ ‘viruses’ or ‘Trojan Horses’.

- Intentionally or carelessly performing an act that places an excessive load on a computer or network resulting in the disruption of the company’s services.
- Failure to comply with requests to discontinue an activity that threatens the operation or integrity of computers, systems or networks.
- Negligently or intentionally revealing passwords or otherwise permitting the use by others of logon accounts for computer and network access.
- Altering or attempting to alter files or systems without authorisation.
- Unauthorised scanning of ports, computers and networks.
- Unauthorised attempts to circumvent data protection schemes, anti-virus software or to uncover vulnerabilities in the company’s security systems.
- Connecting unauthorised equipment to the company's network or computers.
- Attempting to alter any of the company's computing or network components without authorisation or beyond one's level of authorisation, including but not limited to bridges, routers, hubs, wiring, and connections.
- Utilising network or system identification numbers or names that are not assigned for one's specific use on the designated system.
- Using the company's resources to gain unauthorised access to any computer system and/or using someone else's computer without their permission.
- Providing services or accounts on company computers or via the company's networks to other users from a personal computer unless required to meet the normal activities of authorised business.
- Hosting an unauthorised web-site on any of the company’s resources or registering a domain name on any company-owned or leased equipment or utilising any of the company’s IT resources for that purpose unless authorised to do so.
- The connection of ANY device whatsoever [or drivers for such a device] to the company’s IT resources without authorisation – this includes but is not limited to; printers, PDA’s, laptops, standalone or network desktop PC’s.

Authorisation to carry out any of the above must be sought in writing through the IT manager.

Handling of any threats

The safety of people is the highest priority and the first thing to be considered. In the event of any cyber attack, it is imperative that all equipment is made safe. This overrides all other considerations.

Continued operations

When systems and equipment have been made safe, there are further priorities to consider. These are, in order of importance:

- Starting limited, degraded operation where the risk to safety is acceptable, in accordance with usual practice.
- Returning the network to it’s normal state of functioning.
- Taking any remedial action where the point of breach has been identified.
- Identifying, isolating and preserving evidence for forensic analysis.
- Internal investigation into how systems were breached (this must not interfere with any official investigation).
- Remedial action to prevent further breaches.

It is the company’s responsibility to asses and report any attack or threat of attack. At a national level these are split into categories 0-3.

National incidents:

The action required is dependent on the severity of the attack that has taken place. There is a 5-level system (0-3) which indicates correct responses.
Level 0 is divided into 2 sub-levels.

Level 0: Steady State
Level 0: Exceptional Occurrence
Level 1: Significant Emergency
Level 2: Serious Emergency
Level 3: Catastrophic Emergency

Level details can be found in the Cyber Security Guidance to Industry.

Any identified attacks must be raised immediately to the Technical Manager for assessment. In doing so it will be considered based on the following criteria:

- Coincidence with another security breach, perhaps physical
- Records indicating the connection of an unauthorised media or data storage device
- Instructions issued from unexpected sources internally
- Instructions issued from unknown or suspicious sources externally
- Abnormal, illogical or otherwise obviously suspicious instructions being issued from any source
- Recently imported data
- Recent activation of unknown software or script
- Unauthorised disabling of firewalls, or security software
- Unauthorised deletion or alteration of data
- Drops in light levels in fibre-optic cables

Any threat level above Level 0 should be reported immediately in accordance with Cyber Security Guidance to Industry.

Training and communication

Training on this policy forms part of the induction process for all new employees through the Unipart Way online training. All existing employees will receive regular, relevant training on how to implement and adhere to this policy.

Who is responsible for the policy?

The Technical Manager has primary and day-to-day responsibility for implementing this policy, and for monitoring its use and effectiveness as well as dealing with any queries on its interpretation. Management at all levels are responsible for ensuring that those reporting to them are made aware of, and understand, this policy and are given adequate and regular training on it.