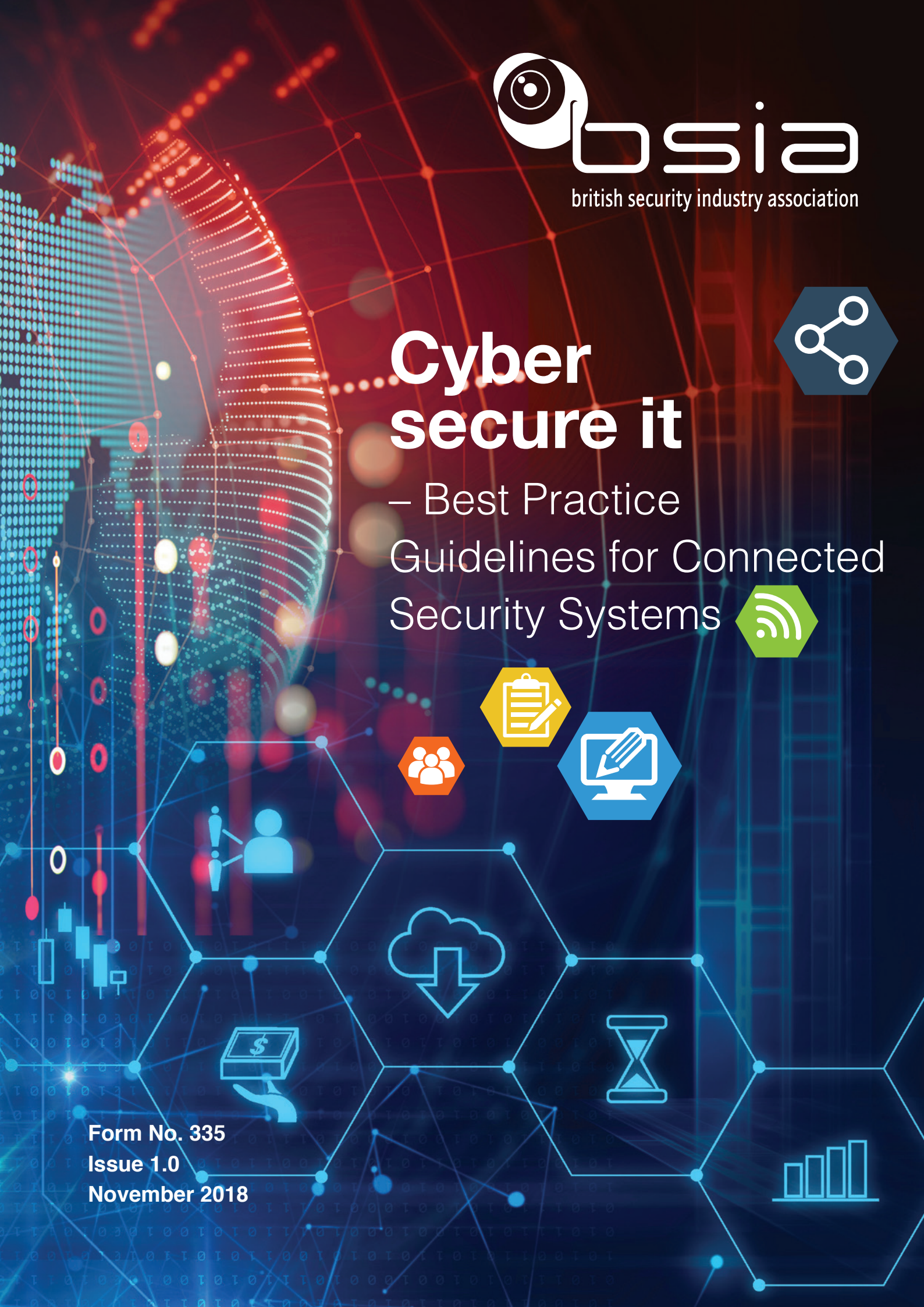


bsia
british security industry association

# Cyber secure it

## – Best Practice Guidelines for Connected Security Systems

Form No. 335
Issue 1.0
November 2018

## Contents

## Terms of Use

This document is intended to be used as a guide by any stakeholder (designers, manufacturers, installers, maintainers, service providers and users) in the supply chain regarding connected security devices/services.

Adherence to the guidance presented in this document does not replace any legal requirements or obligations on the stakeholder, this document is intended to be used as a guide only.

## Copyright

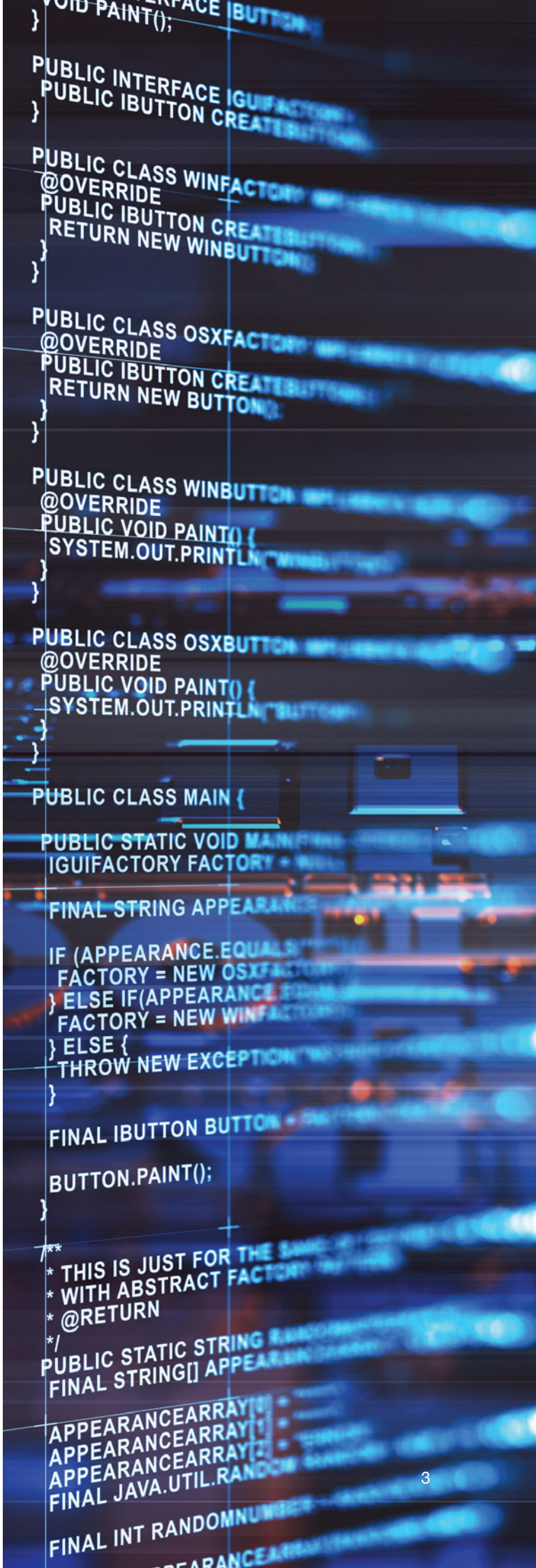


**The British Security Industry Association**
Anbrian House
1 The Tything, Worcester
WR1 1HD

t: 01905 342020 • e: info@bsia.co.uk
**www.bsia.co.uk**

## Acknowledgements

The BSIA acknowledge the assistance given by the BSIA Cyber Security Product Assurance Group (CySPAG) and the following companies for the development of this guide: Bosch Security Systems, Eaton, Horizon Two Six Ltd., ID Cyber Solutions, Securitas, Synetics plc, Tavcom, Thorn Security, UTC Fire & Security UK Ltd., VSG, Webwayone.



## 1 Scope

*This document summarises current guidelines to minimise the exposure to digital sabotage of network connected equipment, software and systems used in electronic security systems.*

It is intended to be used by organisations and stakeholders involved in the manufacture, supply, installation, commissioning, maintenance, and inspection of such systems and also by end users and those involved in remotely monitoring such systems.

Specific guidelines that should be applied as far as possible across the supply chain, are presented covering activities including equipment design, manufacture, installation, maintenance, end use, periodic inspections, remote monitoring and related services.

These guidelines do not cover additional vulnerabilities to which connected security systems may be exposed, for example manufacturing supply chain attacks or social engineering threats, i.e. the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

## 2 Introduction

These guidelines are based on international industry best practice and refer to recognised international guidance and standards.

It is intended that this guidance will provide confidence throughout the supply chain promoting secure connection of products and services, instilling end user confidence in connected security solutions.

This guide will assist the supply chain in their duty of care to other network users, particularly with respect to protecting the integrity of existing cyber security countermeasures already in place or the implementation of such countermeasures in new solutions.

## 3 Document structure

Each section is separately identified for manufacturers, installers, maintainers and remote monitoring. Readers are encouraged to become familiar with all sections of this document, not just the section that relates to their specific interest.

## 4 Terms, definitions and abbreviations

For the purpose of this document, the following terms and definitions apply;

4.1 **Access Point Name (APN)** - the name of a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network, frequently the public Internet. A mobile device making a data connection must be configured with an APN to present to the carrier.

4.2 **Authentication** - verification of the identity of an entity (person/process). See guidance at; https://www.ncsc.gov.uk/guidance/end-user-devices-authentication-policy

4.3 **Authorisation** - A situation whereby an entity (person/process) has permission to access data or to view or make changes to a system

4.4 **Authorised software** - all software applications that form components of the security system including 3rd party applications that form part of the management of the cyber security resilience of the security system, e.g. operating system, antivirus, firewall, software support tools, etc.

4.5 **Confidentiality** - data only available to authorised & authenticated entities (person/process)

4.6 **Configuration data** - data relating to the configuration of the product, any changes to which may impact the security of the product or its key functionality.

4.7 **Data integrity** - The principle whereby data (including software) has not been modified from its original.

4.8 **DeMilitarized Zone (DMZ)** - refers to a host or network that acts as a secure and intermediate network or path between an organization's internal network and the external, or non-propriety network, such as the internet.

4.9 **Encryption** – the process of converting information or data into a code, especially to prevent unauthorised access.

4.10 **Local access** – access by a user physically close to the equipment/system and relies upon the fact that the user must be within the supervised premises. The means of connection to the equipment is irrelevant.

4.11 **Network manager** – The person / organisation responsible for managing the network.
*Note 1: examples of a network manager could be a householder, company IT manager, Security company, Communication provider or ATSP.*

4.12 **Network services** – inbound and outbound connectivity requirements, bandwidth requirements, local connectivity requirements (e.g. DHCP, static addressing).

4.13 **Personal data** –any information relating to an identified or identifiable living individual, as specified in the Data Protection Act 2018, 3(2).

4.14 **Product** –a network connectable device, e.g. a physical device, software or system.

4.15 **Product update lifetime** – period of time or end date which the manufacturer states that the product will be supported for security updates. This will be based on expected threat evolution but new threats may mean that the product cannot be upgraded to protect against these and consequently this update lifetime may need to be reduced.

4.16 **Remote access** – access by a user in any geographical location which does not rely upon the fact that the user must be within the supervised premises. The means of connection to the equipment is irrelevant. There is no physical protection as offered by the supervised premises.

4.17 **Remote centre** –An operation such as an ARC or security control room where remote sessions are instigated and managed.

4.18 **Remote command** – request for information (e.g. status), or command to change the state of the system, originating from a remote access.

4.19 **Remote connection request** – request for remote access wishing to establish a remote connection to the security system or device.

4.20 **Remote device** - an electronic device e.g. PC, tablet or smartphone used to initiate and manage remote connection requests and remote sessions.

4.21 **Remote Session** – period of remote access between successful authentication and disconnection.

4.22 **Security sensitive data** - any critical security parameter that can compromise the security of the device or system, e.g. passwords, keys, seeds for random number generators, authentication data.

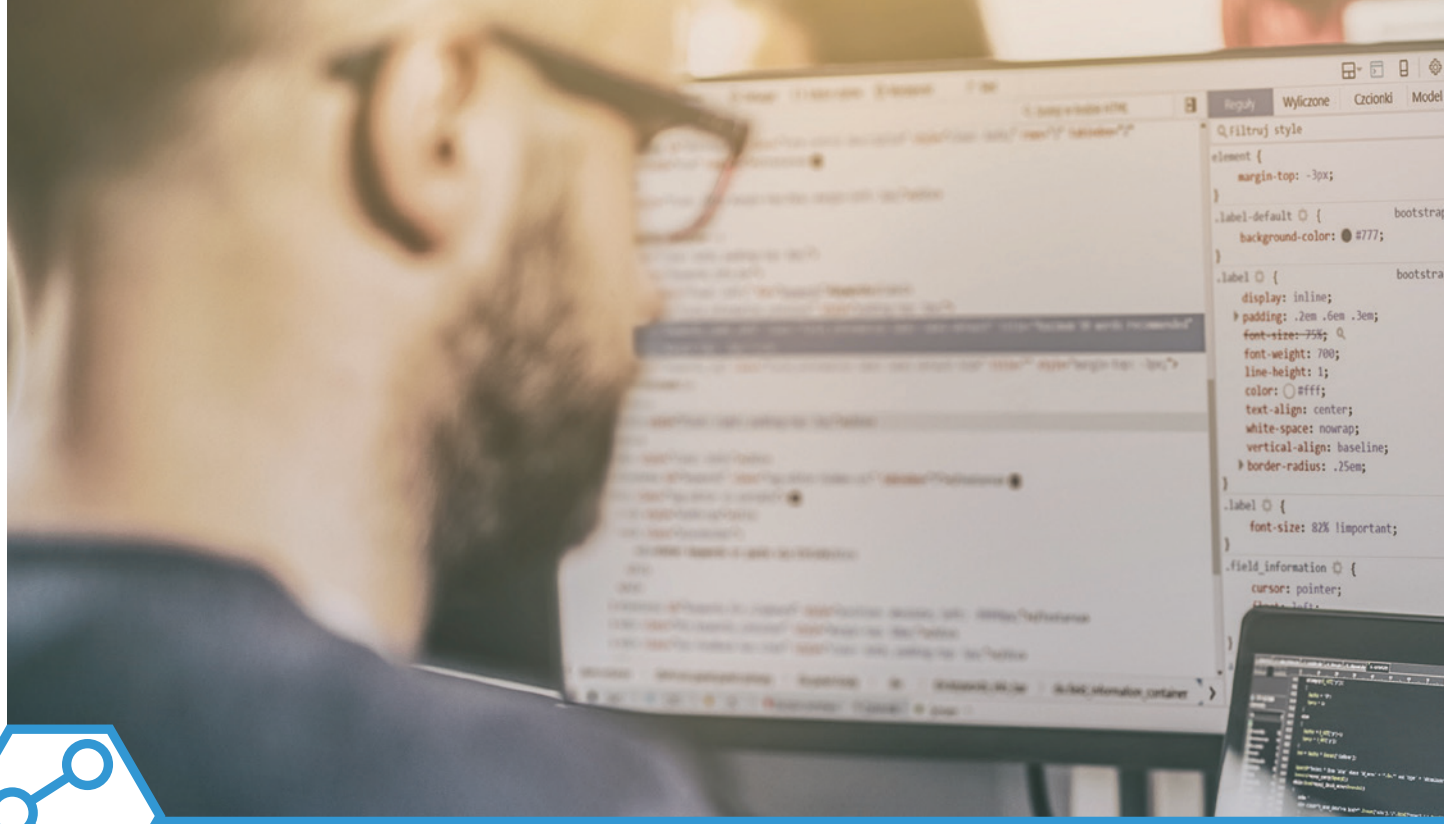
4.23 **Security network** – network and its components used to provide network services between security devices, the security network may be shared or exclusive.

4.24 **Security device** – an element of the security system, e.g. intrusion detection, access control, Video Surveillance Systems, life safety devices, etc. (note: this includes non-dedicated PCs that may be running other business applications).

## Abbreviations

The following abbreviations are used in this document:

| | |
|---|---|
| APN | Access Point Name |
| ARC | Alarm Receiving Centre |
| ATS | Alarm Transmission Systems |
| ATSP | Alarm Transmission Systems Provider |
| BSI | British Standards Institute |
| CAPEC | Common Attack Pattern Enumeration and Classification |
| CESG | Communications-Electronics Security Group |
| CPNI | Centre for the Protection of National Infrastructure |
| CVE | Common Vulnerability and Exposures |
| CVSS | Common Vulnerability Scoring System |
| CWE | Common Weakness Enumeration |
| CWSS | Common Weakness Scoring System |
| CWRAF | Common Weakness Risk Assessment Framework |
| DDoS | Distributed Denial of Service |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | DeMilitarized Zone |
| DoS | Denial of Service |
| GDPR | General Data Protection Regulations |
| ICO | Information Commissioner's Office |
| IP | Internet Protocol |
| LAN | Local Area Network |
| MAC | Media Access Control address |
| NCSC | National Cyber Security Centre |
| NIST | National Institute of Standards and Technology |
| ONVIF | Open Network Video Interface Forum |
| OS | Operating System |
| OWASP | Open Web Application Security Project |
| PC | Personal Computer |
| PIN | Personal Identification Number |
| PnP | Plug and Play |
| RTSP | Real Time Streaming Protocol |
| SANS | The SANS Institute (officially the Escal Institute of Advanced Technologies) |
| SSH | Secure Shell cryptographic network protocol |
| SSID | Service Set Identifier (Wi-Fi network name) |
| SSL | Secure Sockets Layer |
| UL | Underwriters Laboratories |
| USB | Universal Serial Bus |
| VLAN | Virtual Local Area Network |
| Wi-Fi | Wireless Fidelity (wireless networking) |



# 5 Framework Principles

*The following primary principles to manage the cyber security of connected security systems and services underpin the guidance that is contained within this document.*

## 5.1 Priority

5.1.1 Remote connection requests and remote commands should not disrupt the normal primary operations of the system, e.g. to detect, process and notify events.

5.1.2 Commands at the local control equipment should always take precedence over remote commands.

5.1.3 Remote commands should be processed on a first in, first out (FIFO) principle unless a defined message priority or connection is specified by the manufacturer.

5.1.4 Any remote command should be completed before another remote command can change the processing of a preceding command, unless specified differently by the manufacturer.

## 5.2 Remote user authentication and access

5.2.1 As default, users should have minimum privileges (e.g. no remote access) unless increased according to user access requirement needs.

5.2.2 Users accessing the system remotely should be uniquely identified and authenticated (e.g. using passwords, biometrics, certificates, etc.) for audit records of remote access activity and subsequent suspicious behaviour analysis.

5.2.3 Where username and passwords are used for remote user authentication, passwords should be in accordance with www.cyberaware.gov.uk/passwords. *Note: User names and passwords are not the only method of authentication.*

5.2.4 Users remotely accessing the system should be required to provide at least one additional form of authentication over that used for local access, i.e. not via a PIN code alone.

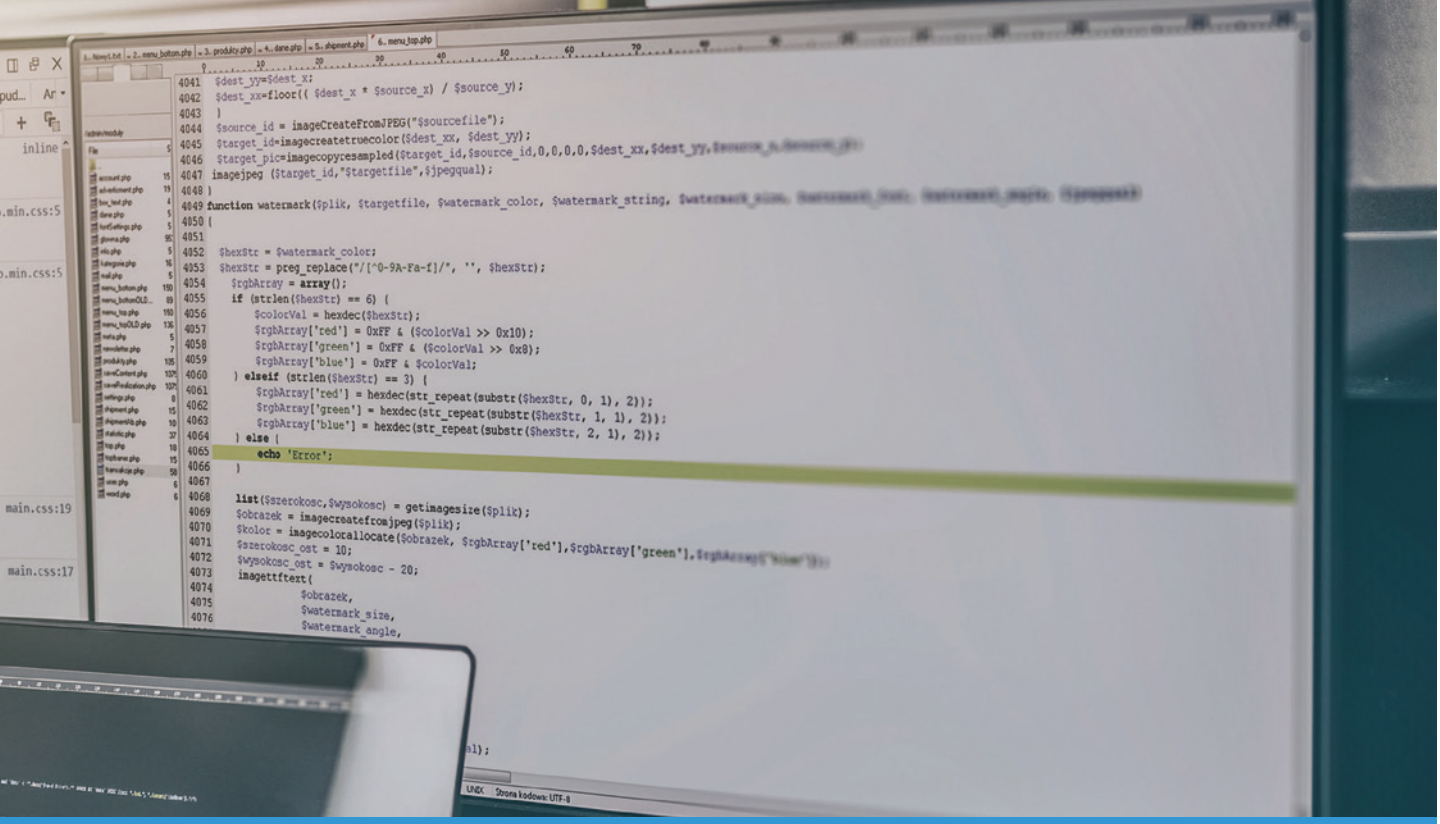
5.2.5 User authentication procedures should be completed prior to the start of each remote session.

5.2.6 Disruption or loss of communications during a remote session should automatically terminate that session. Re-initiation of a failed remote connection should require re-authentication.

5.2.7 The same remote user identity cannot be used for multiple concurrent remote sessions.

5.2.8 Incomplete remote access requests (e.g. login credentials entered but not submitted) should timeout.

5.2.9 Dormant remote access activity for more than 5 minutes should require re-authentication before processing further remote commands.



## 5.3 Management of data integrity

5.3.1 Storage of data on a remote device should be kept to a minimum and should be encrypted.

5.3.2 Data transmitted across a remote connection should be encrypted.

5.3.3 To prevent replay attacks, or modification or substitution of valid remote messages, all data transmitted via a remote connection should be checked for its integrity, for example using the mechanisms described in BS EN 50136-1 in relation to alarm transmission systems.

5.3.4 A decommissioning function should be included to erase/overwrite all configuration and/or personal data.

*Note: Attention is drawn to the General Data Protection Regulations (GDPR) in relation to data security, transmission, storage and deletion.*

## 5.4 Product management

5.4.1 The first use of any product or application should require the change of the default factory username, passwords and/or PINs before use.

5.4.2 Any product firmware and application software should have the ability during its operational lifetime, to be upgraded or updated via a patch to maintain or enhance its cyber security posture; this may be delivered locally or remotely.

5.4.3 Any product firmware or software should have the ability to roll-back any update should it fail to update completely or successfully.

5.4.4 All product or application updates should be validated for their integrity and authenticity before installation.

5.4.5 Download and installation of product or application updates should be planned so as to minimise the disruption to the normal primary operations of the product or application.

5.4.6 The product or application should maintain an event log of all detectable security related events, e.g. successful/unsuccessful logins, change of authentication credentials, changes in user accounts, successful/unsuccessful updates.

5.4.7 The operational lifetime of the product or application should be available in the public domain.

## 5.5 Roles and responsibilities

Responsibility for ensuring the effectiveness of business processes concerning the security of connected products should be clearly defined within each organisation in the supply chain. This should include lineage from executive management through to the end user, including consideration of whole life costs during the life of the system, i.e. maintenance and security updates/patches.

# 6 Guidelines for product

*When undertaking product design, the following should apply;*

## 6.1 Documentation

The following requirement should be documented by the manufacturer:

6.1.1 A product risk assessment and design methodology, commensurate with the assessed threat and consequences, should be conducted to protect against all known applicable cyber security threats.

6.1.2 A design review to verify that the applicable cyber security threats and risks have been considered.

6.1.3 An assessment to determine the product update lifetime.

*Note: This is carried out to determine how long the manufacturer plans to support the product, including updates.*

6.1.4 A process to update manufacturer's knowledge of changing vulnerabilities, weaknesses and exploits.

6.1.5 Regular reviews during the product update lifetime to manage any relevant changing threats, vulnerabilities and weaknesses.

6.1.6 A communication plan for the dissemination of information relating to security and other product updates for the duration of the planned product update lifetime.

## 6.2 Design methodology

The manufacturer should follow a structured design process comprising:

6.2.1 Perform threat modelling (this should encompass both the hardware and software design as appropriate) and document the risk analysis to identify and assess impact of security related threats, exploits and vulnerabilities and eliminate where possible. A list of relevant guidance documents can be found at Appendix A, however risk analysis considerations should as a minimum include;

- attack motivations
- business impact
- threat sources
- system structures
- attack paths
- manufacturing processes

6.2.2 Identify and document vulnerabilities or risks that are determined to have minimal or acceptable impact on the operation of the product that will not be addressed in 6.2.1

6.2.3 Ensure that appropriate tools and mechanisms are included for applying product or application updates.

## 6.3 Verification and validation

6.3.1 Validate that the design (hardware and software) meets the requirements of the risk analysis.

6.3.2 Validation processes should include the following, referring to Appendix A for guidance:

- Use of static code analysis to verify that the code does not contain any weaknesses that might be used for successful exploits.
- Use of structured vulnerability testing to validate effectiveness of risk controls.
- Include deliberate attempts to escalate user privileges.

6.3.3 Consider the use of third party assessment services as appropriate, e.g. ethical hackers, professional test facilities, formal certification (UL, BSI, etc.).

6.3.4 Update risk assessment with results of the validation process and identify any changes to the design that may be required.

6.3.5 Repeat 6.3.1 to 6.3.4 regularly during the product update lifetime in line with a documented review process.

## 6.4 Lifetime product review

6.4.1 Undertake a review of the product for impact of new known vulnerabilities, weaknesses and exploits in line with a documented review process.

6.4.2 Update product design and/or implementation in accordance with the results of the review.

## 6.5 Product documentation

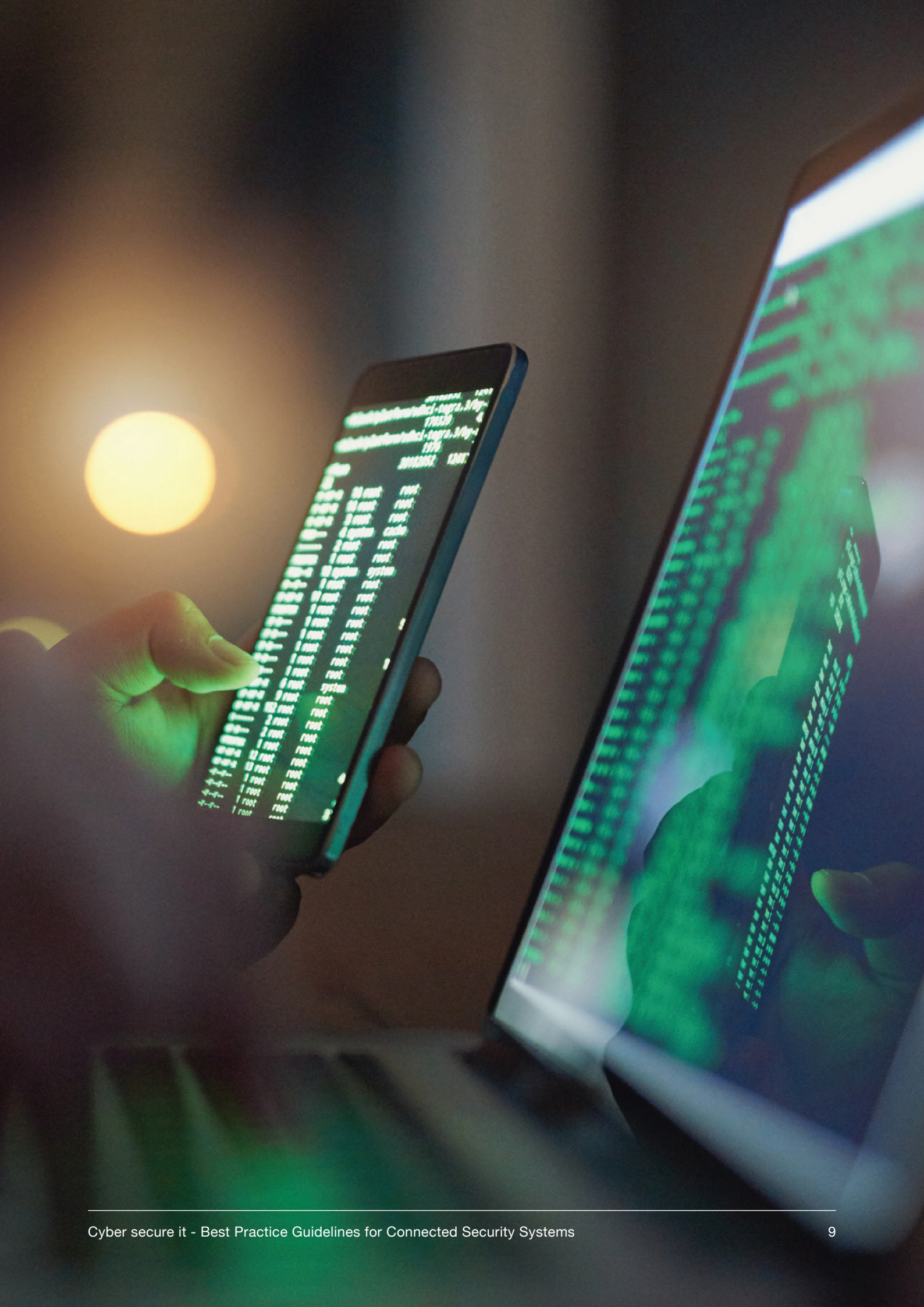
Documentation supplied with the product (in whatever format) should provide support for the activities covered in sections 7 to 11 below, including;

- List of security considerations and "Do's and Don'ts" for system design, installation and use i.e. system level considerations based on how the product is intended to be used (network security, physical access control, firewall ports and protocols, etc.).
- List of consequences regarding impact on the operation of the product if security measures are breached, in line with the risk analysis for proper use of the product.
- List of appropriate tests to be performed to validate correct product commissioning and documentation of such as part of user handover.
- Details of the means by which a product can be updated (e.g. product or application updates) to maintain or enhance its cyber security posture.
- Details of product certification, test certificates and statutory requirements relating to the use of the product.

## 6.6 Communications plan

There should be a documented product support process to include;

- A mechanism to inform system designers, installers and users as appropriate of product or application updates.
- End of product update lifetime and hence continued use may introduce vulnerabilities.




# 7 Guidelines for system installation design

*When undertaking system installation design, the following should apply;*

## 7.1 Objectives

7.1.1 The network configuration should be designed with consideration to the threat modelling and subsequent risk assessment conducted at the installation system design stage.

7.1.2 Ideally the security network should be segregated from any corporate networks, e.g. physical separation or VLAN. This is a layer of security to reduce risk of unscrupulous interaction between security and other site networks.

7.1.3 All security networks containing security devices should be designed with resilience built-in.

## 7.2 Documentation

7.2.1 Security network configuration should be designed for security and documented. This will enable future additional and alterations to the network to be easily managed and tracked.

7.2.2 Network design documentation should include the network services used by the security devices.

7.2.3 The security network should have clearly identifiable, accountable and documented ownership.

7.2.4 The agreed security policies (firmware update procedures, anticipated maintenance life, responsibilities, compliance with host network policies) for maintaining up-to-date cyber security posture of security network equipment should be identified and documented.

7.2.5 The design of the security network should be documented, including;

- records of protocols in use,
- security mechanisms and policies employed,
- permitted access points,
- expansion capability,
- check points,
- the selection of devices to meet the designed minimum security requirements.

7.2.6 Define and record system security policies (e.g. password management, port configurations, etc.) – these may be an extension of existing host network policies.

7.2.7 Consider and document an appropriate level of installed system verification (e.g. structured penetration testing) as defined by the outcome from the risk analysis.

## 7.3 Activities

A structured system design process should be adopted and should as a minimum include the following:

7.3.1 A documented risk analysis should be carried out to identify and assess the impact of security related threats, exploits and vulnerabilities.

7.3.2 Threat modelling should take into account;

- attack motivations
- business impact
- threat sources
- system structures and trust boundaries
- attack paths

7.3.3 Complete a resilience assessment for the security network including;

- consideration of key component failure,
- malicious DoS and/or DDoS attack, etc.

Review degree of resilience against system availability design criteria. Highlight any necessary changes to host network to meet availability design criteria.

7.3.4 Security network configuration ownership and accountability should be formalised, e.g. by department/ individual with nominated deputies.

7.3.5 Consideration of product management policies to keep devices and applications up-to-date should be implemented.

7.3.6 Where it has not been possible to segregate the security network, the security system design should include measures to protect security devices from other network devices.

7.3.7 Where the system utilises Alarm Transmission Systems (ATS), assess the appropriate resilience of the ATS in light of the risk of cyber vulnerability. It is recommended that ATS systems comply with the BS EN 50136 suite of standards.

7.3.8 When using a GSM Cellular network, it is preferred that data should be transmitted over a custom Access Point Name (APN) to segregate this data from the public internet.

7.3.9 Consideration should be given to the adoption of using outbound initiation of communications which will negate the need to open inbound ports on firewalls.

7.3.10 Consideration should be given to ensuring the continuity of access to 3rd party cloud services in the event of changing commercial relationships between installer/ maintainer and cloud service provider, e.g. transfer of system access during takeovers if installer/maintainer ceases trading.

7.3.11 Include all outputs from this initial design assessment within the system design proposal.

# 8 Guidelines for installation and commissioning

## 8.1 Objectives

The following objectives should apply when installing and commissioning any connected security systems;

8.1.1 All default credentials and redundant user accounts should be changed or removed prior to handing over to the client.

8.1.2 Configure security devices and security related devices on the security network to minimise vulnerabilities, e.g. port blocking, port security enabling, use of encryption.

8.1.3 Clients should be fully trained in the use of the system and their responsibilities.

## 8.2 Documentation

8.2.1 Compile, maintain and manage inventory of security devices on the security network in order to be able to actively track device software updates, including a security network diagram showing the security devices connected and other key security related devices, supplied and shared with the network.

8.2.2 Document software applications that are running on the security devices connected to the security network.

8.2.3 Compile, maintain and manage inventory of authorised software applications running on network connected security devices.

8.2.4 Document network configurations and any changes and ensure client has a copy. Explain network changes to the client, if they were not involved in these tasks.

8.2.5 Document the network point of contact to be used by the maintainer, etc. Include these details in the as-fitted security system records.

## 8.3 Activities

8.3.1 Default usernames and passwords (on network security and security related devices) should be changed before handover to the client – if not forced on power-up. Use only strong passwords in accordance with https://www.cyberaware.gov.uk/passwords and in accordance with the site security policy.

8.3.2 A policy should be implemented for the management of passwords.

8.3.3 Any protocols not required should be disabled, e.g. ONVIF streaming, RTSP, web services, PnP, auto-discovery.

8.3.4 Where possible, enable port security on the physical ports of 802.1x switches so that they only respond to devices with configured MAC addresses.

8.3.5 Where possible, enable encryption for all network data traffic in accordance with security network policies.

8.3.6 All security devices should be configured to use the same network time source where available.

8.3.7 Where possible ensure security devices are locked down to only communicate with authorised connections, e.g. whitelisting of connections.

8.3.8 Port configuration:

- Where port forwarding is unavoidable, it is acceptable provided that other security measures are implemented, e.g. SSH, SSL, etc.
- Close all firewall ports by default except those are required for specific device communications.
- Document all ports that are being used and any ports that should be left open – this should be held and maintained by the network manager. It is important that the network manager should NOT close a port that is used by security devices. Equally ports should only be OPENED in accordance with the risk analysis.
- If this is an unmanaged network, e.g. domestic premises, then advice should be given to point out the risks of open and unused ports on a router.

8.3.9 Consider restriction of physical access to servers, other critical network hardware and access points, e.g. check around the security network for open access switches. Where there is open access, provide advice to the host network manager on the security vulnerabilities.

8.3.10 Verify all relevant security network devices have up-to-date software, e.g. by checking devices supplied by the installer, verification from network manager.

8.3.11 Wi-Fi configuration:

- Verify encryption is enabled for any Wi-Fi connections on the security network and is in accordance with the current network security policy.
- It is recommended the Wi-Fi SSID (Service Set Identifier) be configured as hidden.
- Ensure that the Wi-Fi access is password protected, and changed from the manufacturer's default password.
- Confirm that the Wi-Fi connection is to the security network Wi-Fi and not to another network that may be showing as available.

8.3.12 Provide the necessary training to the client, including key client responsibilities to ensure the system remains secure. Ensure the client has a record of any training provided.

8.3.13 There should be an appropriate back-up policy in place and the back-up and restore process should have been tested to recover the system to full operability.

8.3.14 All records regarding the components and configuration settings related to the security network are retained with the as-fitted security system records.

8.3.15 The client should be made aware of the mechanism to advise when security updates are available and how these will be implemented.

8.3.16 The client should be aware of when the product lifetime support will be withdrawn by the manufacturer.

8.3.17 Management policies to ensure devices and applications are up-to-date should be implemented.

# 9 Guidelines for maintenance (by security company)

## 9.1 Objectives

The security company should:

9.1.1 Verify with the client that key system access credentials are up to date, e.g. users with remote access are still authorised.

9.1.2 Ensure that changes in the security network ownership are tracked and communicated to all interested parties.

9.1.3 Ensure the as-fitted security system records are maintained up-to-date with all changes to the system (e.g. device changes, configuration changes). This includes changes arising from planned and unplanned maintenance.

9.1.4 Verify that the security system is operating as originally designed.

## 9.2 Activities

The following activities should be carried out while the engineer is on-site:

9.2.1 Verify with the client that the current password policy has been applied, e.g. passwords updated if required. Consider whether security system remote maintenance access passwords should be changed.

9.2.2 Verify with the client that remote users are still current.

9.2.3 Review the training of client personnel to identify need for refresher or repeat basic training, e.g. due to personnel changes.

9.2.4 Verify with the client back-up procedures are being followed and that any recovery events have been completed successfully.

9.2.5 Review with the client any perceived problems that have been observed with the system which may be indicators of historic or active sabotage activity.

9.2.6 Review and update (if required) the inventory of security devices on the security network; look for anything added or removed, or unused (that should be removed).

9.2.7 Review and update (if required) the inventory of authorised software applications running on network connected security devices.

9.2.8 Verify that there have been no changes to the initial system configuration including:

- all not required protocols remain disabled,
- port security is enabled,
- encryption is enabled,
- all devices use same network time source,
- port forwarding, firewall ports are closed (unless required),
- no new unrestricted physical access to network hardware.

9.2.9 If changes have been made to the system configuration, examine whether these changes have impacted the design assumptions of the initial system design.

9.2.10 Verify the functionality of the security system is operating as originally designed, including receipt of signals or messages at ARCs, where applicable.

9.2.11 Check that all security device updates have been applied.

9.2.12 Review security system and Alarm Transmission Systems (ATS) event logs for evidence of suspicious/ abnormal behaviour, e.g. multiple failed remote access attempts or excessive transmission faults.

9.2.13 Where used, verify the white list of authorised connections is up-to-date and valid.

9.2.14 Identify on-going cyber related problems and effect their resolution.

9.2.15 Check that network ownership and contact records are up-to-date.

9.2.16 Check the client is aware of the mechanism used to advise when security updates become available and how these will be implemented.

9.2.17 Check the client is aware of the mechanism used to advise when product lifetime support will be withdrawn by manufacturer.

9.2.18 Update the as-fitted security system records, as necessary.

# 10 Guidelines for remote monitoring and maintenance

*This section covers the infrastructure and the operational procedures for remote monitoring and maintenance, e.g. ARCs, in-house control rooms, installer premises, etc.*

**A security system may be connected to a remote centre for a number of reasons, including but not limited to:**

- **Monitoring of and response to alarm signals**
- **System control, e.g. setting / unsetting**
- **Planned and reactive remote maintenance activities**

## 10.1 Objectives

When connecting a security system to a remote centre ensure that the connection does not in any way degrade the cyber security posture of the system, i.e. the connection must not increase the risk of the security system being subject to a cyber-attack. This may be achieved by considering two main areas:

- Infrastructure hardening, e.g. use of firewalls, OS patch updates, application patch updates, use of antivirus measures.
- Management of remote centre personnel, e.g. appropriate security screening, training, monitoring and management of their activities in relation to the security systems.

## 10.2 Activities

10.2.1 Remote centres should have a process to confirm applications, engineering tools and software which are used to connect to security systems are maintained and up-to-date with all released security updates.

10.2.2 Remote centres should consider compliance with minimum IT security best practice as defined within Cyber Essentials https://www.cyberessentials.ncsc.gov.uk/advice/.

10.2.3 Consider best practice of hosting internet facing devices, e.g. hosting receivers in a DMZ and only allowing traffic to flow to/from whitelisted devices, whilst denying all traffic for everything else.

10.2.4 Firewalls should be configured to allow only ports needed by the devices through to the receiver in the DMZ, then on a separate rule to allow the receiver to forward that signal into the LAN. A rule to 'deny all' traffic not specifically configured to be allowed should be added as the last rule to close everything else.

10.2.5 Remote centres which can access security systems should reside on a physically separated network or VLAN, so as to reduce the opportunity for cyber-attacks to take place on the remote centre network.

10.2.6 Appropriate measures should be taken to restrict physical access to devices and applications capable of connecting to security systems to only remote centre personnel .

10.2.7 Client PC's and server equipment operating in a remote centre should have up-to-date antivirus software installed, and this should be correctly configured.

10.2.8 Internet access for remote centre personnel should be restricted by whitelist to only those websites which are required to carry out their jobs. The whitelist should be reviewed on a six monthly basis as a minimum and any websites which are no longer required to be accessed should be removed.

10.2.9 Where possible, USB ports should be disabled on all devices within the remote centre to mitigate the risk of a virus being introduced via a mass storage device. Where it is necessasary for operational reasons to allow the use of USB ports, these ports should be physically secured and access controlled, e.g. locked in a secure cupboard or comms room.

10.2.10 Where appropriate and possible, consideration should be given to the use of VPNs to secure any IP link between the remote centre and the security system.

10.2.11 A policy should be in place to ensure that passwords for all systems used by remote centre personnel accessing security systems are in accordance with the advice given at https://www.cyberaware.gov.uk/passwords . Passwords and accounts used by staff who have left the business are deleted expediently.

10.2.12 Remote centres should ensure that all personnel are screened in accordance with BS 7858. Remote centre personnel should not be given access to equipment which has the ability to remotely access a security system until security screening has been successfully completed.

10.2.13 Remote centre personnel who have the ability to remotely access security systems should receive training in cyber security principles, so that they understand as a minimum the types of security measures in place, the need for these measures and the potential consequenses of the measures being reduced or removed. Training should be documented and signed of by each staff member and the trainer, to indicate that the employee has attained a suitable level of competence in the subject.

10.2.14 The activities of remote centre personnel should be appropriately monitored to enable an audit trail to be established. This should enable actions taken by remote centre personnel either unitentionally or maliciously which increase the level of security risk, to be detected and rectified.

# 11 Guidelines for users (i.e. client/ user responsibility)

## 11.1 Objectives

These guidelines are intended to assist the user where the user has agreed to take responsibility, as defined in the system design proposal, for managing the routine operation of the security network or system. The following responsibilities should be clearly defined and assigned:

- Maintain and manage an inventory of security devices on a security network.
- Maintain and manage an inventory of authorised software applications running on security related devices.

Prepare and test contingency plans, specifically a cyber security incident response plan for actions on detection of a breach.

## 11.2 Activities

Where the client/user has assumed responsibility, the following activities should be undertaken by the client/user (where applicable).

11.2.1 A password policy should be implemented and consistently applied.

11.2.2 The security system should be maintained up-to-date in line with security updates issued by the manufacturer/installer/maintainer/3rd party.

11.2.3 All users of the security system should be instructed in its correct use, particularly with respect to cyber related issues.

11.2.4 All users of the system should be current, particularly those with remote access credentials.

11.2.5 The installer/maintainer of the security system should be advised of security network changes that may impact the cyber security posture of the security system.

11.2.6 Perform a risk assessment on the consequences of a security breach on the security system or security network, e.g. images collected from surveillance cameras, user passwords stolen, etc. For risks that are not acceptable, prepare and test contingency plans to deal with each event. Plans should include immediate actions, persons to contact, software update procedures, device isolation, investigation into extent of breach.

11.2.7 Ensure that an effective data back-up policy is in place and has been tested.

# 12 Contingency Planning

Each stakeholder (designers, manufacturers, installers, maintainers, service providers and users) in the supply chain should have robust and appropriate contingency planning measures in place that should address where a breach has or is likely to occur or where vulnerabilities become known. This document does not cover how to manage these issues, simply to remind stakeholders that contingency plans should be implemented and regularly tested.

# 13 References

**List of references, as cited above.**


- BS EN 50136 - Alarm transmission systems and equipment. suite of standards
- Data Protection Act 2018
- General Data Protection Regulations (GDPR)


**Other useful references:**


- CESG Architectural Patterns 10 - Serving Web Content – issue 1.1 Oct 15 - NCSC Web.pdf
  Note: This government document gives guidance on internet hosting;
- The Information Commissioner's Office (ICO) – http://www.ico.org.uk/
- Centre for the Protection of National Infrastructure (CPNI) – www.cpni.gov.uk
- The National Cyber Security Centre (NCSC) – www.ncsc.gov.uk
- Cyber Essentials – https://www.cyberessentials.ncsc.gov.uk


# Appendix A

**References to Security Design Methodologies for Applications**


1. Common Weakness Risk Assessment Framework (CWRAF)
2. Common Weakness Enumeration (CWE), ITU-T X.1524
3. Common Weakness Scoring Scheme (CWSS), ITU-T X.1525
4. Common Attack Pattern Enumeration and Classification (CAPEC), ITU-T X.1544
5. Common Vulnerability and Exposures (CVE), ITU-T X.1520
6. Common Vulnerability Scoring (CVSS), ITU-T X.1521
7. OWASP Top 10 vulnerabilities
8. OWASP Project
9. NIST National Vulnerability Database
10. CWE/SANS top 25 software errors

## About the BSIA

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

**www.bsia.co.uk/sections/information-destruction**

---

## For further information please contact:


**BSIA, Anbrian House**

**1 The Tything, Worcester WR1 1HD**

**t: 01905 342020**

**e: info@bsia.co.uk**

**www.bsia.co.uk**


bsia

british security industry association