Installation of safety and security systems
Cybersecurity code of practice

Important information

This code of practice does not purport to include all the necessary provisions of a contract.

Users of this code of practice are responsible for its correct application.

Compliance with this code of practice cannot confer immunity from legal obligations.

For other information please contact:

British Security Industry Association

01905 342 020
info@bsia.co.uk
www.bsia.co.uk

Contents

1. Introduction

Safety and security systems having connections to internal and external networks have increased exposure to malicious attack. To assure the achievement of effective cybersecurity requires that these types of systems be appropriately designed, installed, commissioned and maintained.

It is intended that this code of practice will assist in providing confidence throughout the supply chain promoting secure connection of products and services, delivering client assurance regarding connected solutions.

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

This code of practice sets out the logical order in which systems would normally be addressed in terms of cybersecurity. Each process is set out separately in the guidelines, but it is accepted that, in practice, some of the processes may be carried out simultaneously or in a different order.

The recommendations of this code of practice apply in addition to other standards and codes of practice relating to systems and equipment to be installed. Any documentation or checklists mentioned in this code of practice may be combined with those required by the other standards or codes of practice.

This code of practice applies to safety and security systems and their components but could be applied to other devices and systems.

2. Scope

This code of practice provides recommendations on how to minimise the exposure to digital sabotage of installed devices, applications and systems, for the protection of safety and security and the utilised network.

This document provides cybersecurity recommendations for the design, planning, operation, installation, commissioning and maintenance of installed devices, applications and systems with a cyber exposure.

It is intended to be useful for organisations and stakeholders involved in the installation, commissioning and maintenance, of such systems and also for the client and those involved in remotely monitoring such systems.

Each stakeholder (designers, installers, maintainers and clients) in the supply chain should have robust and appropriate contingency planning measures in place that should address where a cyber-attack has or is likely to occur or where vulnerabilities become known. This code of practice does not cover how to manage these issues, simply to remind stakeholders that contingency plans should be implemented and regularly tested.

The following are not considered to be within the scope of this code of practice; network monitoring, contingency planning and installed devices/systems with no cyber exposure, manufacturing supply chain vulnerabilities and social engineering.

3. Terms, definitions & abbreviations

3.1. Terms and definitions

For the purposes of this code of practice, the following terms and definitions apply:

3.1.1. Allow list

A list of systems, devices, applications ports or protocols that have been approved, i.e. all entities are denied access, except those included in the allow list.

3.1.2. Client

Individual or corporate body responsible for acquiring the installed system.

3.1.3. Commissioning

Putting an installed system into operational mode.

3.1.4. Critical security update

A security update issued in response to an exploit being discovered and requiring urgent installation.

3.1.5. Deny list

A list of systems, devices, applications ports or protocols that have been blocked, i.e. all entities are allowed access, except those included in the deny list.

3.1.6. Encryption

The process of converting information or data into a code, especially to prevent unauthorised access.

3.1.7. Exploit

Means by which a cybersecurity flaw or weakness within a device or application is used to gain malicious access to, or control of, the device or application.

3.1.8. Installed application

A software element of the installed system, e.g. an application running on a PC (or other electronic device) for monitoring, control or configuration of a system.

3.1.9. Installed device

A physical element of the installed system including device firmware and software provided by the manufacturer, e.g. control equipment, detection devices, visual imaging devices, viewing devices, dedicated PCs, notification devices etc.

3.1.10. Installed system

A system of devices and applications designed for safety or security. e.g. intrusion detection, access control, video surveillance systems, life safety systems (fire detection or fire suppression systems), social care systems.

3.1.11. Installing organisation

Organisation responsible for the design, installation or maintenance process.

3.1.12. Nominated person

A person(s) or organisation(s) formally nominated by the client to undertake assigned responsibilities (see 5.2) in relation to the cybersecurity of an installed system.

Terms, definitions & abbreviations

3.1.13. Remote access

Access to the installed system at a supervised premises by an authorised user from any geographical location for the purposes of interrogating or operating the system.

3.1.14. Secure network protocol

A type of network protocol that ensures the security and integrity of data in transit over a network connection. Network security protocols define the processes and methodology used to secure network data against any illegitimate attempt to review or extract the contents of data.

3.1.15. Security update

A software update supplied by the manufacturer for a device or application that provides protection against cyber vulnerabilities or enhances cybersecurity.

3.1.16. Security update support

Support for security updates for devices or applications provided by the manufacturer.

3.1.17. Vulnerability

A cybersecurity flaw or weakness within a device or applications that may expose a device or application to a threat.

3.2. Abbreviations

For the purposes of this code of practice, the following abbreviations apply.

FTP File Transfer Protocol

IPSec Internet Protocol Security (a secure network protocol suite)

LAN Local Area Network

ONVIF Open Network Video Interface Forum

PC Personal Computer

PnP Plug and Play

RTSP Real Time Streaming Protocol

SSID Service Set Identifier

Telnet Telecommunications network (network virtual terminal protocol)

VLAN Virtual Local Area Network

4. Installing organisation – general

Systems should be installed, operated and maintained in a manner to maintain the cybersecurity in accordance with the recommendations of this code of practice and, where applicable, the client's policies and standards. Where any part of the client's policy has been used as an alternative to the recommendations of this code of practice, this should be documented and agreed with the client.

Note: *As part of an overall cybersecurity strategy it is recommended that installing organisations consider a scheme such as Cyber Essentials. For more information visit www.ncsc.gov.uk.*

4.1. Confidentiality

Information and documentation relating to the design, installation, operation and maintenance of the installed system should be treated as confidential and stored securely.

4.2. Competence

Persons responsible for the design, installation planning, system installation, maintenance and repair of the installed system should have the appropriate training and/or experience in cybersecurity. Individual records of all training received should be retained and subject to regular review.

4.3. Security policy

The installing organisation should always maintain and apply a security policy. This is a documented policy outlining how to protect the organisation from cybersecurity threats.

5. Responsibility

The responsibility of maintaining and applying cybersecurity of an installed system is shared across the manufacturer, installing organisation and the client.

Note: *Attention is drawn to BSIA Form 343 - Manufacturers of safety and security systems - Cybersecurity code of practice.*

Responsibility for each individual stage in the process of system design, installation, commissioning, hand-over and maintenance should be clearly defined and agreed between the relevant parties.

Where an organisation takes responsibility for the ongoing installation/maintenance of an existing installed system, it is the responsibility of this organisation to carry out the necessary activities to meet the recommendation of this code of practice, e.g. where appropriate documentation is not available.

5.1. Client

The client should assume the responsibilities of the nominated person or nominate a person who will have the authority for the activities described below in clause **5.2**. Where the activities have been assigned to other organisations or people, formal notification of this assignment should be issued to each organisation or person(s) and a copy retained by the installing organisation.

The installing organisation should not assume responsibilities for the role of the nominated person.

5.2. Nominated person

For any installed system, the nominated person is responsible for (see **6.8**):

a) Following and applying the system cybersecurity policy (see **6.1**)
b) Allowing security updates to be applied to the installed system (see **6.5**)
c) Informing the installing organisation about any network changes in accordance with the communications plan (see **6.6**)
d) Ensuring all users of the installed system are trained in line with their role(s), including how their actions can impact the cybersecurity of the installed system (see **6.7**)
e) Ensuring the agreed maintenance schedule is followed (see **6.9**)
f) Informing the installing organisation in the event of any indication of a malfunction, cybersecurity breach or physical damage (visible or suspected) to any part of the installed system

5.3. Installing organisation responsibilities

For any installed system, the installing organisation is responsible for the activities below. Where the activities have been assigned to other organisations or people, formal notification of this assignment should be issued to each organisation or person(s) and a copy retained by the installing organisation.

a) Creating, maintaining and consistently applying the following at the appropriate stage during the lifetime of each installed system:
- System cybersecurity policy (see **6.1**)
- Training record (see **6.7**)
- Nominated person acceptance (see **6.8**)
- Maintenance schedule (see **6.9**)
- Design survey for cybersecurity (see **6.10**)
- System design (see **6.11**)
- As fitted records (see **6.12**)

b) Following any relevant additional client security policy requirements.
c) Only installing devices and applications that claim compliance to the requirements of *BSIA Form 343 - Manufacturers of safety and security systems - Cybersecurity code of practice*. Or, where a manufacturer does not claim compliance for devices and/or applications, the installing organisation should perform due diligence by completing a check according to **ANNEX E**.
d) Installing devices and applications securely and in accordance with the manufacturer's recommendations. If this is not possible or unclear, advice should be sought from the manufacturer or supplier.
e) Ensuring that all software and hardware installed can be verified as being supplied by trusted sources, e.g. manufacturers or approved partners.
f) Registering as appropriate with each device manufacturer or application supplier to ensure receipt of all security updates, critical security updates and changes to security update support.

g) In the event of a security update being issued by the manufacturer for an installed device or application, the installing organisation should notify the nominated person and with their agreement implement and verify the security update in a timely manner. Critical security updates will require immediate action.

h) Where notified of the withdrawal of security update support for an installed device or application the installing organisation should advise the client that no further updates can be supplied which may reduce the protection against vulnerabilities and exploits, and then advise the client on appropriate options.

Note: *As cybersecurity threats are continually evolving, the protection against these can be software, hardware or a combination of both. It may not be possible to protect against new threats with software only updates. If it is not possible to protect against new threats, then the manufacturer may withdraw security update support for the installed device or application.*

i) When notified of a suspected or confirmed cybersecurity incident the installing organisation should:

- review the impact of the incident on the cybersecurity of the installed system.
- review the system cybersecurity policy.
- review the system design.
- take appropriate action(s).

6. Documentation

The documentation listed within this section should be completed and maintained for each system at the appropriate stages. Where similar documentation already exists then the requirements from this section may be merged into the existing process or documentation.

6.1. System cybersecurity policy

A system cybersecurity policy is a document outlining how to protect the system from known and evolving cybersecurity threats to the installed system and what action(s) should be taken.

Where specific elements of a system cybersecurity policy (listed below) already exists at the site and covers the requirements of this code of practice then the site policy will take priority and where this has been adopted it should be noted in this policy.

The system cybersecurity policy should cover **6.2** to **6.6** as a minimum.

6.2. Roles and responsibilities register

Schedule of assigned and agreed roles and responsibilities related to the ongoing correct operation of the cybersecurity of the installed system.

6.3. Back-ups

Details the back-up and restore processes enabling system recovery to full operability in the event of data loss and methodology used to test these processes.

6.4. Passwords

Requirements for passwords should be applied in line with advice from the **National Cybersecurity Centre.**

Note: *requirements for password policies should be based on risks to the installed system and cover the management of the passwords, for example what happens when an employee leaves the organisation.*

6.5. Updates

Process employed to apply both security updates and critical security updates. This should include the maximum permitted time to install a security update or critical security update following receipt of notification and how the updates will be applied. Consideration should be given to any customer supplied equipment, for example a PC running installed applications.

6.6. Communications plan

Plan detailing how the installing organisation and nominated person will communicate when notifying of events related to the cybersecurity of the installed system. This should include contact details and the types of events that will be covered by the plan.

Note: *for example, the installing organisation notifying the nominated person of a security update or the nominated person notifying the installing organisation of changes to the network such as disabling of firewalls, removal of encryption, opening of closed ports, replacement of router.*

6.7. Training record

A documented record of the training provided to those identified in the roles and responsibility register.

6.8. Nominated person acceptance

A documented record of acceptance of the installed system and associated responsibilities.

6.9. Maintenance schedule

A documented schedule as agreed by all parties, to ensure the continued correct functionality and cybersecurity of the installed system.

Note: *The frequency of cybersecurity maintenance activities may differ from other system maintenance activity.*

6.10. Design survey for cybersecurity

A survey to inform the system design of decisions to be taken on the cybersecurity of the installed system (see **ANNEX A**).

6.11. System design

A document to describe the design of the system that should address the needs of the client, describing the functional and cybersecurity requirements of the proposed installed system.

The system design should include details on the architecture of the proposed installed system and include the following:

- Details of the proposed installed devices and/or applications e.g. manufacturer, model, type.
- Network topology (see **ANNEX D** for guidance)
- Details of any network devices that the installing organisation are taking responsibility for e.g. routers, switches, firewalls.
- Any protocols and services required by the proposed installed devices or applications, for example: ONVIF streaming, RTSP, web services, PnP, auto-discovery, Telnet, FTP.
- Encryption method to be used for connections for all the proposed installed devices and applications (wired and wireless).
- Permitted actions from a remote location by a user.
- The remote access interfaces for system administration.
- Planned network segregation of installed devices and applications from any devices not part of the installed system, e.g. physical separation or VLAN (where practicable).

6.12. As fitted records

All records regarding the components and configuration settings related to the installed system should contain the following:

6.12.1. Cybersecurity installation check sheet

A documented check list used by the installing organisation to confirm that cybersecurity best practices have been applied to the installed system (see **ANNEX B** and **ANNEX C**).

6.12.2. Deny and allow list inventory

A documented record of any installed devices or applications that have been placed on a deny list or allow list, as necessary. Where deny or allow listing is not used then this inventory is not required.

6.12.3. Installed applications inventory

A documented inventory of installed applications that comprises the system with the primary focus of being able to actively track installed application software updates.

6.12.4. Installed devices inventory

A documented inventory of installed devices that comprises the system with the primary focus of being able to actively track installed device software updates.

6.12.5. Installed network configuration

A document detailing the network configurations, including the network type, and any network equipment and ports in use.

6.12.6. System verification

A document detailing the installed system verification results as defined in the system design.

7. System Design

The objectives of the system design are to determine the functional and cybersecurity requirements of the installed system, to determine the architecture and components necessary to meet these requirements, and to document the solution agreed with the client.

The following activities should be undertaken by the installing organisation:

a) Complete the design survey for cybersecurity (**ANNEX A**)
b) Create the system cybersecurity policy (see **6.1**)
c) Create the maintenance schedule (see **6.9**)
d) Create the system design (see **6.11**)
Note: *this could be included in the overall system design*
e) Gain written acceptance of the system design, the system cybersecurity policy and maintenance schedule from the client and/or nominated person.

8. Installation and commissioning

The objectives of this stage are to install and commission the system according to the system design utilising cybersecurity best practice.

The installing organisation should:

a) Install the system in accordance with the system design.
b) Review and agree any outstanding items from the cybersecurity installation check sheet, in writing, with the nominated person.
c) Agree any deviations from the system design, in writing, with the nominated person. The system design should be updated to highlight any agreed changes.
d) Create as fitted records (see **6.12**).
Note: *this could be included in the overall system as fitted records*
e) Complete the cybersecurity installation check sheet (see **ANNEX B** and where appropriate, **ANNEX C**)
f) Commission and verify that the system is installed in accordance with the system design. Any failures should be resolved prior to progressing to the handover and acceptance stage.

9. Handover and acceptance

The objectives of the handover and acceptance stage are to ensure that the nominated person is provided with the necessary information and training in order to manage and operate the installed system cybersecurity through the agreed processes and responsibilities.

The following activities should be undertaken by the installing organisation:

a) Provide the nominated person with training to ensure the ongoing correct operation of the installed system and make sure that the nominated person understands:
- the security update support mechanism, in accordance with the system cybersecurity policy; and,
- how security updates and cybersecurity related matters will be communicated, in accordance with the system cybersecurity policy; and,
- accepts the responsibilities of the nominated person.

b) Gain written acceptance (and record) from the nominated person of the installed system.

10. Maintainance

The objective of the maintenance stage is to ensure the continued cybersecurity of the installed system. The installed system should be maintained according to the agreed maintenance schedule.

The following activities should be undertaken by the installing organisation (either locally or remotely) in accordance with the maintenance schedule:

a) Review installed system event logs for evidence of suspicious/abnormal behaviour, e.g. multiple failed remote access attempts or excessive transmission faults and take appropriate actions.

b) Review with the nominated person any perceived problems that have been observed with the installed system which may be indicators of historic or active sabotage activity and take appropriate actions.

c) Review and update the system cybersecurity policy. Any changes should be agreed, in writing, with the nominated person.

d) Review and update the cybersecurity installation check sheet based on how the installed system is being used, in particular looking for any changes. Any changes should be agreed, in writing, with the nominated person, or rectified as required.

e) Verify that the installed system is operating in accordance with the as fitted records and perform any necessary actions.

f) Review and update the training record as appropriate and provide training where required.

g) Record all activities carried out during this maintenance visit, including any changes to the installed system and, where appropriate, update as fitted records. Obtain formal agreement and acceptance of these activities and changes from the nominated person.

Note: *In the event of a corrective maintenance visit some of the above may be appropriate for fault identification.*

Annex A: design survey for cybersecurity – mandatory

This checklist refers to the cybersecurity arrangements and may be combined with those required by the other standards or codes of practice relating to security and safety systems and equipment.

The design survey for cybersecurity should cover the following as a minimum:

No.	Check	Y/N	Comments
1	Could a nominated person be identified now? If yes, record contact details?		
2	Is there a contact for IT/Cyber/network issues? If yes, record contact details?		
3	Does the client have an IT policy(s) which covers cybersecurity?		
4	Do these policies impact the design and installation of the system?		
5	Are there any specific testing requirements?		
6	Does the client have a roles and responsibilities register?		
7	Does the client have a back-up policy?		
8	Does the client have a passwords policy?		
9	Does the client have a communications plan for reporting cyber incidents and updates?		
10	Will the installed system be utilising a dedicated network?		
11	Will the installed system be utilising a shared network (managed)?		
12	Will the installed system be utilising a shared network (un-managed)?		
13	Is there a list of network equipment (e.g. routers, firewalls, switches, cabling) that will be supplied by the client?		
14	Are there specification(s) available for any network equipment that will be supplied by the client?		

***Note**: this questionnaire is related specifically to cybersecurity and other questions related to IT or network capability may be covered in other documentation.*

Annex B: cybersecurity installation checksheet – mandatory

The checks and comments are mandatory however the format is for guidance only. If the check is not applicable to the installed system, then the answer should be 'NA' with justification entered into the comment column.

This checklist refers to the cybersecurity arrangements and may be combined with those required by the other standards or codes of practice relating to security and safety systems and equipment.

No.	Check	Y/N/NA	Comments (if the answer is No or NA)
1	Confirm that the configuration for each installed device or application is in accordance with manufacturer guidance.		
2	Confirm there is a record of configuration for each installed device/application included as fitted records so that it can be verified where unauthorised changes have taken place.		
3	Have all default usernames and passwords (for all admin and other user levels) been changed?		
4	Have all redundant user accounts been removed or disabled?		
5	Have all user accounts been set to lowest level of privileges, e.g. all accounts are non-admin, and only system administrators have admin access?		
6	Confirm that all security updates have been applied to all relevant installed devices, applications and system(s).		
7	Confirm that any protocol and services not required have been disabled for the installed devices or applications, e.g. ONVIF streaming, RTSP, web services, PnP, autodiscovery, Telnet, FTP.		
8	Are all installed devices and applications time synced, for example, where available, SNTP or NTP?		
9	Confirm that encryption has been configured for connections for all installed devices and applications (wired and wireless). ***Note:*** *consideration should be given to the encryption technique used, as some techniques offer greater protection.*		
10	Confirm that wireless networks have the SSID changed to one that is not obviously associated with company / site, and to not broadcast the SSID.		
11	Confirm that the network is configured so that installed devices and applications are segregated from any devices not part of the installed system, e.g. physical separation or VLAN (where required by the system design).		
12	Confirm that port forwarding is not being used or where port forwarding is required by the system design, confirm that all other firewall ports have been closed except those chosen to be used in the system.		
13	Confirm that installed devices have been entered in the installed devices inventory.		
14	Confirm that installed applications have been entered in the installed applications inventory.		
15	Confirm that where remote access is used, that it only uses agreed secure protocols and services.		
16	Confirm that all software and hardware installed can be verified as being supplied by trusted sources, e.g. manufacturers or approved partners.		

Annex C: cybersecurity installation checksheet – advisory

The checks and comments are advisory and may be added to the check sheet in Annex B.

If the check is not applicable to the installed system, then the answer should be 'NA' with explanation entered into the comment column.

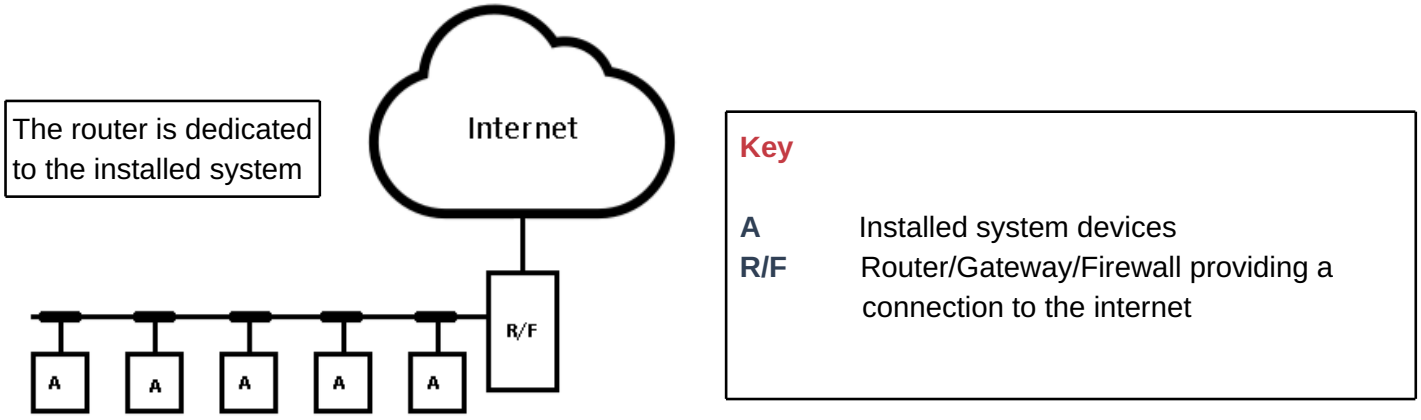
No.	Check (in accordance with appropriate policies)	Y/N/NA	Comments (if the answer is No or NA)
1	Confirm that the router / switch and firewall are configured to prevent unauthorized connections by default.		
2	Confirm that port security is enabled on the physical ports of 802.1x switches.		
3	Confirm the default 'Deny All' firewall feature has been enabled.		
4	Confirm that the 'secure network protocol' feature has been configured for encrypting communication within the network(s) e.g. IPSec.		
5	Confirm the 'intrusion detection' firewall feature has been enabled.		
6	Confirm the 'logging' feature has been enabled in the router /firewall/switch, especially for all log-in attempts (both successful and failed).		
7	Confirm that only agreed remote access interfaces for system administration have been enabled, all others are disabled.		

Annex D: network types – informative

Network types incorporate all forms of network infrastructure, e.g. Ethernet, Wi-Fi and 4G. The risks will be different depending on the network types listed below:

Dedicated network

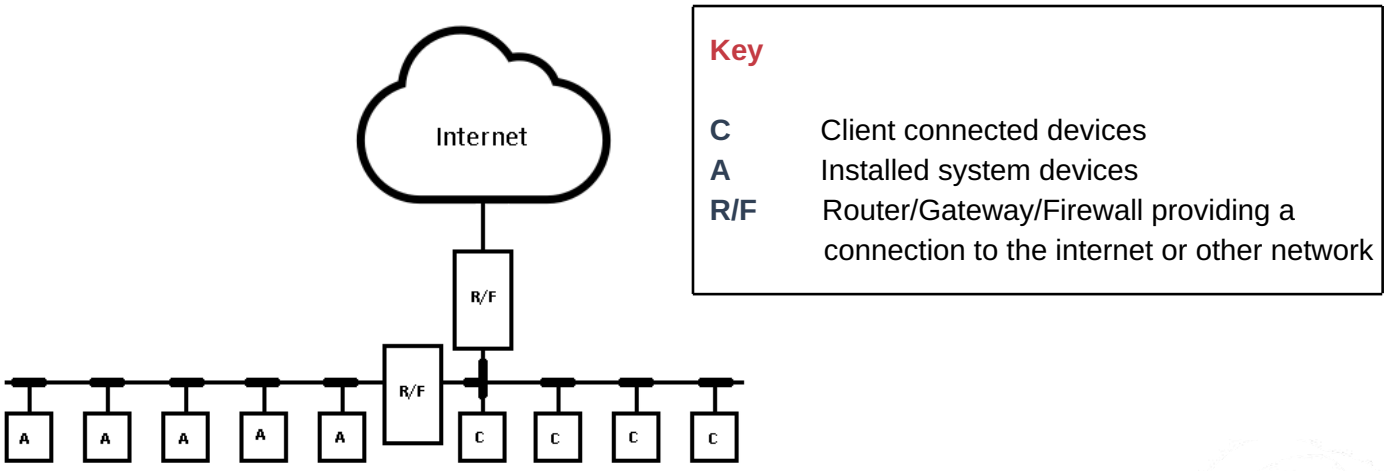
A dedicated network is a network that only contains devices and applications provided by, or installed and maintained by, the installing organisation. This will incorporate a method to ensure it is physically segregated from other networks. This network will have a formal management and maintenance programme that is provided by the installing organisation.



Segregated network

A segregated network is a network that only contains devices and applications provided by, or installed and maintained by, the installing organisation. This will incorporate a method to ensure it has a defined boundary and is physically separated up to the point it connects into the clients' network, where there is a virtual separation. The segregated part of the network will have a formal management and maintenance programme that is provided by the installing organisation.

Note: *the separation of installed system network(s) and client network(s) can be achieved in more than one way e.g. using a VLAN or a device with independent unbound network interface connections.*

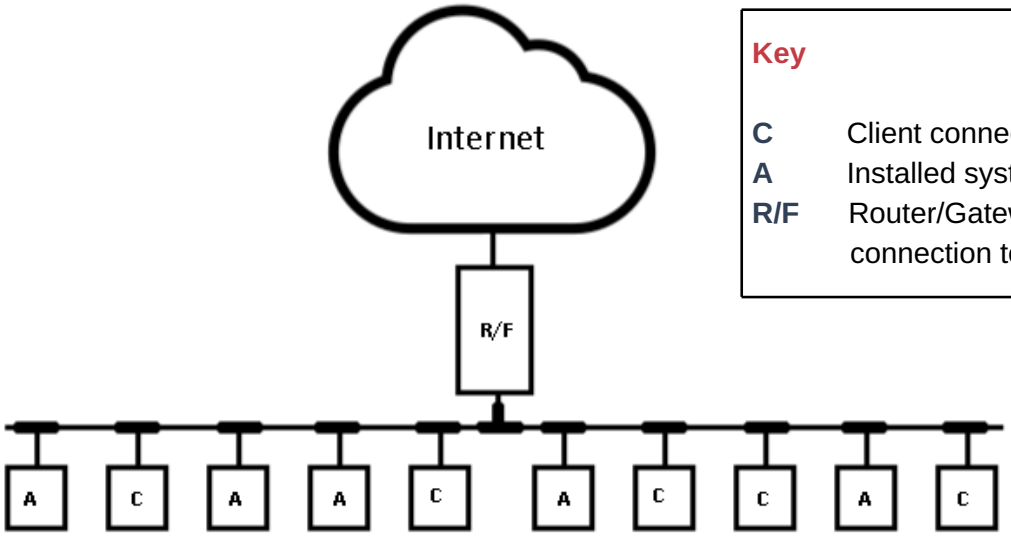


Annex D continued: network types – informative

Shared network

Managed: a shared managed network is a network that contains devices and applications in addition to those installed and maintained by, the installing organisation. The network will have a formal management and maintenance programme that is provided by the client.

Unmanaged: a shared unmanaged network is a network that contains devices and applications in addition to those installed and maintained by, the installing organisation. This network will have no formal management or maintenance programme in place.



Key

C	Client connected devices
A	Installed system devices
R/F	Router/Gateway/Firewall providing a connection to the internet or other network

Annex E: due diligence for a device or application – mandatory

This code of practice requires that manufacturers either claim compliance to the requirements of BSIA Form 343 *Manufacturers of safety and security systems - Cybersecurity code of practice* or provide the information requested in the check list below. This checklist refers to the cybersecurity specific measures.

A manufacturer of a cyber resilient device or application should be able to provide the information requested below. If the manufacturer is unable to provide any of the information, then careful consideration should be given before using the device or application and a mitigation plan recorded in the comments section.

No.	Check	Response from manufacturer/comment
1	What is the manufacturer's communications plan for security updates?	
2	What is the manufacturer's communications plan for critical security updates?	
3	What is the manufacturer's communications plan for withdrawal of security update support?	
4	How does the manufacturer supply advice and support for how to install products securely?	
5	How does the manufacturer supply advice and support for how to implement security updates?	
6	How does the manufacturer supply advice and support for how to verify if software and hardware supplied is from a trusted source?	
7	How does the manufacturer provide a method for installers or interested parties to report suspected or confirmed cybersecurity incidents (vulnerability disclosure)?	

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.

This code of practice was produced by the **Cybersecurity Product Assurance Group (CySPAG)** of the BSIA who would like to acknowledge the assistance given by the following organisations in the development of this code of practice:

Eaton
FIA
Horizon Two Six Ltd
IoTSF Smart Buildings Working Group
Johnson Controls
NSI
SSAIB