Form_342:2020_draft_20200415

Installation of safety and security systems - Cyber security code of practice

May 2020

For other information please contact:

British Security Industry Association
t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk

Document history

Date	Issue	Comment
XX May 2020	1.0	First Issue

Contents

1. Introduction

This code of practice is based on international industry best practice regarding cyber security and refers to recognised guidance and standards as it applies to safety and security systems.

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 cyber security 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 cyber security. 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.

Although this code of practice focusses on safety and security systems and its components, there may be other devices and systems this code of practice could be applied to, although those devices and systems are outside the scope of this code of practice.

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.

2. Scope

This code of practice aims to minimise the exposure to digital sabotage of installed devices, applications and systems with a cyber exposure, for the protection of safety and security. This provides recommendations on the design, planning, operation, installation, commissioning and maintenance of installed devices, applications and systems with a cyber exposure.

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

This code of practice does not cover additional vulnerabilities to which these installed devices, applications and 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.

Each stakeholder (designers, 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 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; alarm transmission systems, network monitoring, contingency planning and installed devices/systems with no cyber exposure.

3. Terms, definitions and abbreviations

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

3.1. Terms and definitions

3.1.1. Blacklist
A blacklist is a list of items that are blocked access to a certain systems, ports or protocols.

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 software update for a device or application that provides cyber security patches that have been provided in response to an exploit being discovered.

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

3.1.6. Exploit
A cyber security flaw or weakness within a device or applications that does expose a device or application to a threat.

3.1.7. 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.

3.1.8. 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 devices, viewing devices, dedicated PCs etc.

3.1.9. 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.

3.1.10. Installer
Individual or individuals responsible for carrying out the installation process.

3.1.11. Installing organisation
Installing organisation responsible for the design, installation or maintenance process.

3.1.12. Nominated person
A person or organisation formally nominated by the client to undertake assigned responsibilities.

3.1.13. 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.

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

3.1.15. Security update

A software update for a device or application that provides cyber security patches or enhancements as part of ongoing improvements by the manufacturer.

3.1.16. Security update support

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

Note: Support from the manufacturer may be withdrawn and no further updates supplied which may reduce the protection against vulnerabilities and exploits.

3.1.17. White list

A whitelist is a list of items that are granted access to a certain systems, ports or protocols. When a whitelist is used, all entities are denied access, except those included in the whitelist.

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
Wi-Fi	Wireless Fidelity (wireless networking)

4. Installing organisation - general

Systems should be installed, operated and maintained in a manner to maintain the cyber security in accordance with the recommendations of this code of practice that does not expose the system or the network to any new or additional risks that were not there before the installation.

Installation should be in accordance with the client's policies and standards and recommendations of this code of practice, or just this code of practice.

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.

Note: Attention is also drawn to data protection legislation in relation to personal data.

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 experience in cyber security.

4.3. Organisation security policy

The installing organisation should always maintain and apply an organisation security policy, this is a documented policy outlining how to protect the organization from cyber security threats.

Note: it is recommended that installing organisations obtain cyber essentials, for more information visit www.cyberessentials.ncsc.gov.uk.

5. Responsibility

The responsibility of maintaining and applying the cyber security of an installed system is spread across the manufacturer, installing organisation and client.

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.

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 delegated to other organisations or people, it should be documented.

5.2. Nominated person

For any installed system, the nominated person is responsible for the following.

a) Follow and apply the system cyber security policy (see 6.1)
b) Ensuring the agreed maintenance schedule is followed (see 6.4)
c) Allow the installing organisation access (locally or remotely) to the installed system in order to apply security updates.
d) Inform the installing organisation about any network changes that may impact the cyber security of the installed system, e.g. disabling of firewalls, removal of encryption, opening of closed ports, replacement of router.
e) Ensure all users of the installed system are trained to the appropriate level of access and how their actions can impact the cyber security of the installed system.
f) Inform the installing organisation in the event of any indication of a malfunction, cyber security breach or damage to any part of the installed system.

5.3. Installers responsibilities

For any installed system, the installer is responsible for the activities below. Where the activities have been delegated to other organisations, it should be documented.

a) Creating, maintaining and consistently applying the following at the appropriate stage for each installed system:
   - System cyber security policy (see 6.1)
   - Training record (see 6.2)
   - Nominated person acceptance (see 6.3)
   - Maintenance schedule (see 6.4)
   - System design (see 6.5)
   - As fitted records (see 6.6)

b) Follow any relevant additional client security policy requirements.

c) Only install devices and applications that claim compliance to the requirements of BSIA Form no. 343 'Manufactures of safety and security systems - Cyber security code of practice'.

d) Where a manufacturer does not claim compliance for a devices and/or application, the Installer should check with the manufacturer and obtain written confirmation of what cyber security measures the manufacturer has employed for the selected devices and/or applications.

   Note: If a manufacturer is unable to supply information about the cyber security measures in place then the devices and/or application should be considered high risk and it is strongly recommended that it is not installed.

e) Install 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.

f) Ensure that all software and hardware installed can be verified as being supplied by genuine sources, e.g. manufacturers or approved partners.

g) Subscribe to the manufacturers method of communicating security updates, critical security updates and changes to security update support.

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

i) Where notified of the withdrawal of security update support for an installed device or application the installer 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.

j) Supply the client with advice relating to the effective cyber security management of the installed system.

k) When notified of a suspected or confirmed cyber security incident the installer should:
   - review the impact of the incident on the cyber security of the installed system.
   - review the system cyber security 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 cyber security policy

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

Where specific elements of a system cyber security 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 cyber security policy should cover the following as a minimum:

6.1.1. Design cyber security survey

A survey to inform the design that enables decisions to be made on the cyber security of the installed system design. (see

Annex A - Design cyber security survey – Normative)

6.1.2. Roles and responsibilities register
Schedule of assigned and agreed roles and responsibilities related to maintaining the cyber security of the installed system.

6.1.3. Back-ups
Details the back-up and restore processes to recover the system to full operability in the event of loss of data and how this process is tested.

6.1.4. Passwords
Requirements for passwords in use on the installed system. This should be applied in line with advice from the National Cyber Security Centre - https://www.ncsc.gov.uk/collection/passwords

6.1.5. Updates
Process employed to apply both security updates and critical security updates. This should include expected timescales and how the updates will be applied.

6.1.6. Communications plan
Plan detailing how the installing organisation and nominated person will communicate when notifying of events related to the cyber security 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 installer of changes to the network such as disabling of firewalls, removal of encryption, opening of closed ports, replacement of router.

6.2. Training record
A documented record of nominated persons or installed system users trained in the use of the installed system appropriate to their level of responsibility and access.

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

6.4. Maintenance schedule
A documented schedule which is agreed by all parties, to ensure the continued correct functioning and cyber security of the installed system.

Note: The frequency of cyber security maintenance may be different to other system maintenance activities.

6.5. System design
A document to describe the design of the system that should address the needs of the client.

The system design should contain the following wording (or words to the effect of):

To ensure the ongoing cyber security of the installed system and as part of this design the client will either assume the responsibilities of the nominated person or nominate a person or organisation to assume the following responsibilities:

- *Follow and apply the system cyber security policy.*
- *Ensure the agreed maintenance schedule is followed.*
- *Allow the installing organisation access (locally or remotely) to the installed system in order to apply security updates.*
- *Inform the installing organisation about any network changes that may impact the cyber security of the installed system, e.g. disabling of firewalls, removal of encryption, opening of closed ports, replacement of router.*

- *Ensure all users of the installed system are trained to the appropriate level of access and how their actions can impact the cyber security of the installed system.*
- *Inform the installing organisation in the event of any indication of a malfunction, cyber security breach or damage to any part of the installed system.*

It is recommended that the client or nominated person visits National Cyber Security Centre website (www.ncsc.gov.uk) for guidance on cyber security responsibilities.

6.6. As fitted records

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

6.6.1. Black and white list inventory

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

6.6.2. 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.

6.6.3. 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.

6.6.4. Installed network configuration

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

6.6.5. System verification

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

6.6.6. Cyber security installation check sheet

A documented check list used by the installer to confirm that cyber security best practices have been applied to the installed system. (see Annex B – Cyber security installation check sheet – Normative)

7. System design

The objectives of the system design stage are to determine the extent of the installed system and select devices and/or applications with the appropriate level of cyber security functionality/performance and document the system design.

The following activities shall be undertaken by the installer:

a) Create the system cyber security policy.
b) Create the system design.

Note: this could be included in the overall system design

c) Create the maintenance schedule.
d) Gain written acceptance of the system design, the system cyber security 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 cyber security best practice.

The installer should:

a) Install the system in accordance with the system design.
b) Review and agree any outstanding items from the cyber security 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 6.6).

Note: this could be included in the overall system as fitted records

e) Complete the cyber security installation check sheet (Annex B – Cyber security installation check sheet – Normative)
f) Commission and verify the system is installed in accordance 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 maintain the installed system cyber security through the agreed processes and responsibilities.

The following activities shall be undertaken by the installer.

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 cyber security policy; and,
    - how security updates and cyber security related matters will be communicated, in accordance with the system cyber security policy; and,
    - accepts the responsibilities of the nominated person.
b) Gain written acceptance (and record) from the nominated person of the installed system.

10. Maintenance and repair

The objective of the maintenance and repair stage is to ensure the continued cyber security of the installed system. The installed system should be maintained according to the agreed maintenance schedule.

The following activities should be undertaken by the installer (either locally or remotely):

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 cyber security policy. Any changes should be agreed, in writing, with the nominated person (only on a maintenance visit).
d) Review and update the cyber security 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.
e) Verify that the installed system is operating in accordance with the as fitted records and perform any necessary actions.
f) Gain acceptance (and record) for the activities carried out on the installed system from the nominated person.

Annex A - Design cyber security survey – Normative

The design cyber security survey should cover the following as a minimum:

No.	Check	Y / N	Comments
1	Is there a contact for IT/Cyber/network issues?		
2	Could a nominated person be identified now? If so, who is it?		
3	Does the client have an IT policy(s) which covers cyber security?		
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 communication 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 cyber security and other questions related to IT or network capability may be covered in other documentation.

Annex B – Cyber security installation check sheet – Normative

No.	**Check** (in accordance with appropriate policies)	Y / N	**Comment** (required if the answer is 'No' or if the check is not applicable)
1	Confirm that the configuration for each type of device (router, switch, firewall, or installed device) is in accordance with manufacturers guidance for that device and/or network		
2	Have all default usernames and passwords (for all admin and other user levels) have been removed or replaced?		
3	Have all redundant user accounts have been removed or disabled?		
4	Have all user accounts are set to the lowest level of privileges, e.g. all account are non-admin accounts, and that only system administrators have admin access		
5	Confirm that latest security updates have been applied to all relevant installed devices, applications and system(s)		
6	Confirm that any protocol and services not required have been disabled, as well as unsecure protocols and services (for example: ONVIF streaming, RTSP, web services, PnP, auto-discovery, Telnet, FTP)		
7	Are all installed devices and applications configured to use the same network time source (where available)		
8	Confirm that the highest possible level of encryption has been configured for connections for all installed devices and applications (wired and wireless) by default		
9	Confirm that wireless networks have the SSID changed to one that is not obviously associated with company / site, and to not broadcast the SSID		
10	Confirm that installed devices and applications have been segregated from any devices not part of the installed system, e.g. physical separation or VLAN (where practicable)		
11	Confirm that port forwarding is not being used		
12	Where port forwarding is required by the system, confirm that all firewall ports have been closed by default except those that are required by the system and documented		
13	Confirm that the router / switch and firewall are configured to prevent unauthorized connections by default		
14	Confirm that port security is enabled on the physical ports of 802.1x switches		
15	Confirm that installed devices have been entered in the installed devices inventory.		
16	Confirm that installed applications have been entered in the installed applications inventory.		
17	Confirm the default 'Deny All' firewall feature has been enabled		
18	Confirm that the 'secure network protocol' feature has been configured for encrypting communication within the network(s) e.g. IPSec		
19	Confirm the 'intrusion detection' firewall feature has been enabled		
20	Confirm the 'logging' feature has been enabled in the router / firewall / switch, especially for all log-in attempts (both successful and failed)		
21	Confirm that only agreed remote access interfaces for system administration has been enabled, all others are disabled by default		
22	Confirm that where remote access is used, that it only uses agreed secure protocols and services		
23	Confirm that there is a record of the configuration so that it can be verified where unauthorised changes have taken place		
24	Confirm that all software installed has been supplied by genuine sources, e.g. manufacturers or approved partners.		

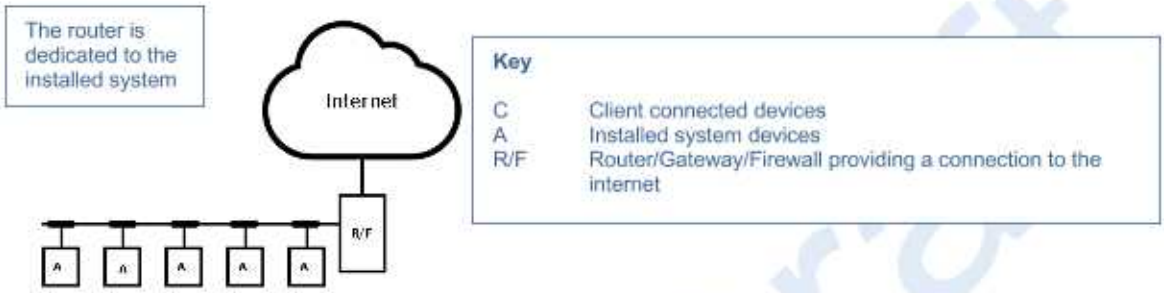
Note: The checks and comments are mandatory however the format is for guidance only. If the check is 'not applicable' then the answer should be 'no' with justification entered into the comment column.

Annex C - 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

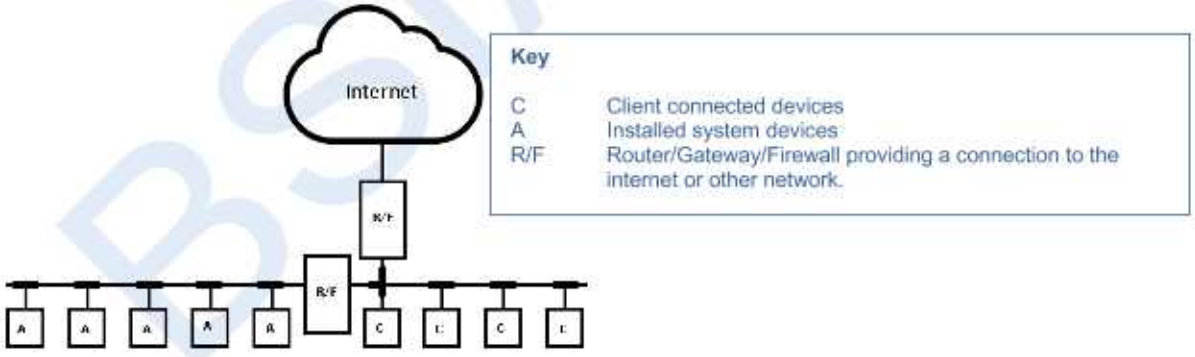
A dedicated network is a network that only contains devices and applications provided by, or installed and maintained by, the installing organisation. This will incorporate a method to ensure it is physically segregated from other networks. This network will have a formal management and maintenance programme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

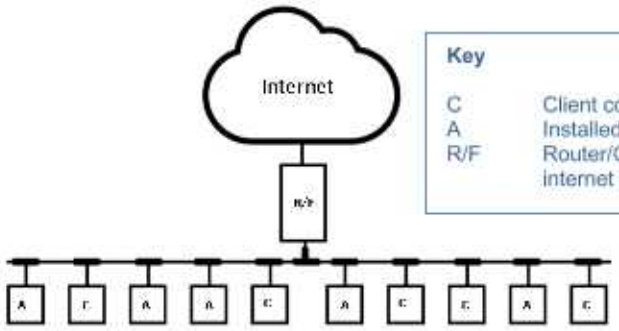
Note: The separation of installed system network(s) and client network(s) can be achieved in more than one way e.g. using a VLAN or a device with independent unbound network interface connections.



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.

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 Cyber Security Product Assurance Group (CySPAG) of the BSIA who would like to acknowledge the assistance given by the following companies in the development of this code of practice: ……

BSIA Ltd
Anbrian House
1 The Tything
Worcester
WR1 1HD

t: 01905 342 020
e: info@bsia.co.uk
www.bsia.co.uk