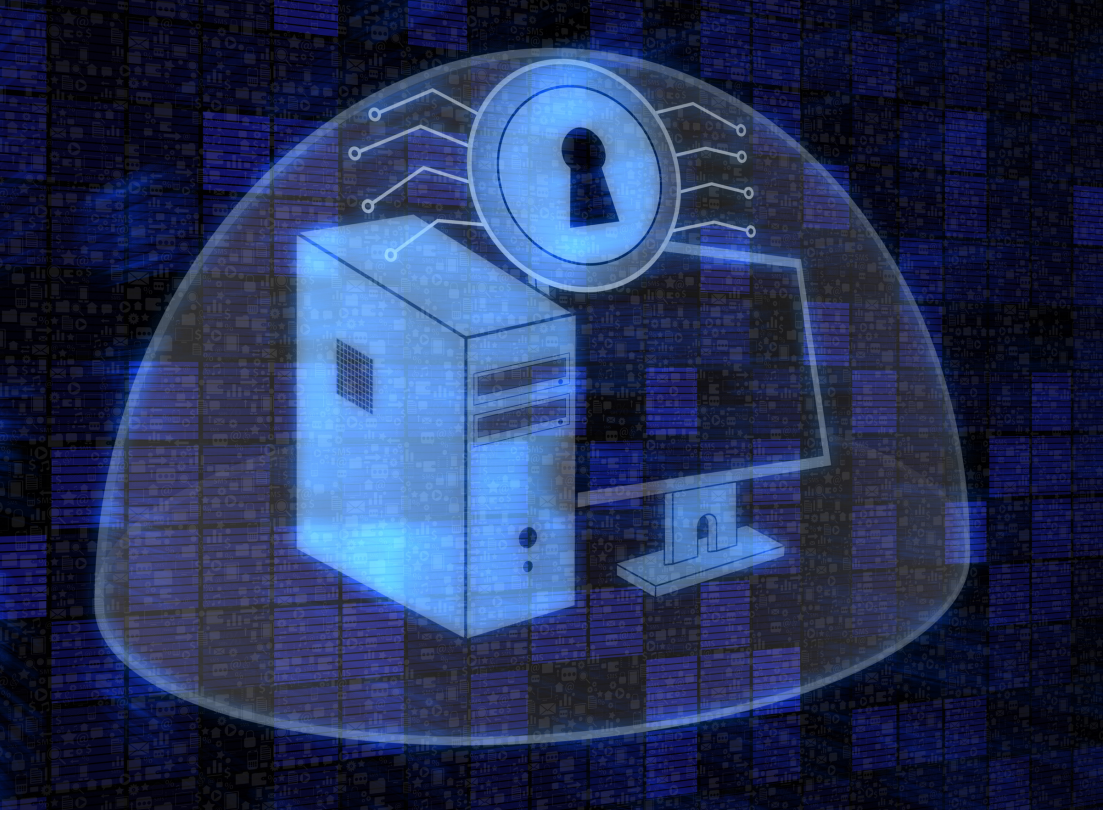

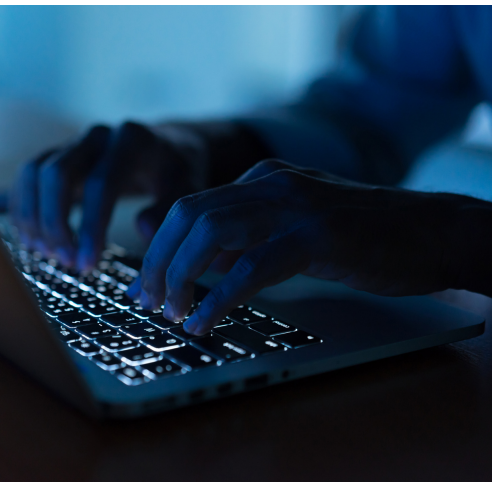

Manufacturers of safety and security systems

Cybersecurity code of practice

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association

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.

Contents

1. Introduction

This code of practice is based on international industry best practice regarding cybersecurity 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 cybersecurity countermeasures or the implementation of such countermeasures in new solutions.

Although this code of practice focuses on safety and security products, there may be other products this code of practice could be applied to, although those products are outside the scope of this code of practice.

This code of practice contains common cybersecurity terminology. Where the reader is unfamiliar with these terms other resources should be consulted, for example, as cited in Annex A.

2. Scope

This code of practice provides recommendations on the design, testing and manufacture of safety and security products with a cyber exposure.

It is intended to be used by manufacturers involved in the design, testing and manufacture of such products.

This code of practice does not cover additional vulnerabilities to which these products may be exposed, for example 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.

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

It is recommended that each stakeholder (manufacturer, designer, installer, maintainer, service provider and user) in the supply chain should consider the need for robust and appropriate contingency planning measures 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.

3. Terms, definitions & abbreviations

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

3.1. Client

Individual or corporate body responsible for acquiring the installed system.

3.2. Credentials

A set of attributes that uniquely identifies a system entity such as a person, an organisation, a service, or a device.

3.3. Critical security update

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

3.4. Exploit

An input or action intended to take advantage of a weakness (or multiple weaknesses) that negatively impacts a product.

Note: *The existence of an exploit targeting a weakness is what makes that weakness a vulnerability.*

3.5. Product

A device, service, application or system designed for safety or security. e.g. intrusion detection, access control, video surveillance systems, social alarms, life safety systems.

3.6. Remote access

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

3.7. Security update

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

3.8. Security update support

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

Note: *As cybersecurity threats are continually evolving, the protection against these can be software, hardware or a combination of both. Software-only updates may not be sufficient to protect against new threats. If it is not possible to protect against new threats, the manufacturer may withdraw security update support. If no further updates are supplied this may reduce the protection against vulnerabilities and exploits.*

3.9. Vulnerability

A software weakness found in the product for which an exploit exists such that it can be directly used by an attacker.

3.10. Weaknesses

An error in the architecture, design, coding, build process or configuration of software, that may render a product vulnerable.

4. Manufacturing organisation – general

A product should be designed and supported in a manner to maintain its cybersecurity in accordance with the recommendations of this code of practice.

4.1. Confidentiality

Information and documentation relating to the design of a product should be treated as confidential and stored securely.

4.2. Competence

Persons involved in design, testing and manufacture of a product should have appropriate current training and experience in cybersecurity.

4.3. Organisational security policy

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

Note: *it is recommended that a manufacturer obtains Cyber Essentials Plus certification or equivalent, for more information visit www.ncsc.gov.uk/cyberessentials/overview.*

5. Responsibility

The responsibility for maintaining and applying cybersecurity for a product is shared across the manufacturer, installing organisation and the client.

Responsibilities for the installing organisation and clients can be found in *BSIA Form 342 - Installation of safety and security systems - Cybersecurity code of practice*.

For any product, the manufacturer is responsible for the following.

a) Designing products to be cyber secure in accordance with this code of practice.
b) Operating processes to keep up to date with changing weaknesses, exploits and vulnerabilities.
c) Performing regular reviews during the period of security update support to manage any relevant changing weaknesses, exploits and vulnerabilities.
d) Maintaining a communications plan in order to provide a method of communicating the following to the supply chain:

- security updates
- critical security updates
- withdrawal of security update support.

e) Providing advice and support in relation to:

- how to install products securely
- how to implement security updates
- how to verify that software and hardware supplied is genuine.

f) Maintaining a vulnerability disclosure policy.

6. Documentation and policies

The documentation listed within this section should be completed and maintained for each product at the appropriate stages.

6.1. Design documentation

The design documentation should comprise a record of the structured design process, to include the following as detailed in section 7:

a) Threat modelling.
b) Risk analysis.
c) Vulnerability and risk identification.
d) Design validation.
e) Product review.

6.2. Communications plan

There should be a documented product support process to inform the supply chain of the following:

a) Security updates.
b) Critical security updates and the associated risk if not applied.
c) Date of withdrawal of security update support, including the reason for withdrawal and the associated risk if no action is taken. Where withdrawal of security update support is due to planned end of life, the manufacturer should allow sufficient time for the supply chain to react.

6.3. Vulnerability disclosure policy

This is a documented policy that defines the method for interested parties to report suspected or confirmed cybersecurity incidents. There should be a public point of contact to enable interested parties to report issues. Where a vulnerability is disclosed the manufacturer should act on this in a timely manner, based upon the associated risk.

Note: *A "timely manner" is dependent upon the disclosed vulnerabilities and the impact that they may have on the product. The ETSI EN 303 645 recommended time to handle a disclosed vulnerability is within 90 days.*

7. Design methodology

The manufacturer should follow a structured design process as detailed below.

Note: *A list of sources of useful information can be found at Annex A.*

7.1. Threat modelling

Perform threat modelling (this should encompass both the hardware and software design as appropriate).

7.2. Risk analysis

Undertake a documented risk analysis to identify and assess impact of security related threats, exploits and vulnerabilities. The risk analysis should as a minimum consider:

a) Attacker motivations.
b) Business impact.
c) Threat sources.
d) System structures.
e) Attack paths (inbound and outbound).
f) Manufacturing processes.
g) Third party libraries.

7.3. Vulnerability and risk identification

Identify and document any vulnerabilities or risks that may have an impact on the operation of the product.

Product design or mitigation controls used to address the identified vulnerabilities or risks should be documented.

Any identified vulnerabilities or risks that will not be addressed, as they have been determined to have minimal or acceptable impact on the operation of the product, should also be documented with a justification for not addressing them.

7.4. Design of mitigation controls

Design and implement effective mitigation controls appropriate to the product and its deployment context to address the risks and vulnerabilities identified in **7.3.**

7.5. Design validation

Validate that the design (hardware and software) meets the requirements above (**7.4**). Processes should include the following:

a) Use of static code analysis to verify that the code does not contain any known vulnerabilities.
b) Use of structured vulnerability testing and input fuzzing (e.g. using generational and template based malformed inputs) to validate effectiveness of risk mitigation controls.

c) Deliberate attempts to escalate user privileges.
d) Any other relevant method of test.

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

Note: *Consider the use of third-party assessment services as appropriate, including professional penetration testers registered with the UK Cyber Security Council, professional test facilities, formal certification (e.g. BSI, UL).*

7.6. Product review

Repeat the above (**7.1** to **7.5**) regularly during the security update support period in line with the documented product review process.

8. Product design requirements

8.1. General requirements

8.1.1. Defaults

Product defaults must not allow access to an existing system until suitable authorisation has been established.

There should be either:
• No universal factory set default credentials, or;
• First time use credentials

Where the product does not contain universal factory default credentials the product should prompt the user to create credentials.

Where the product contains first time use credentials (universal factory default credentials) the product should enforce the change of those credentials on that first use.

8.1.2. Event log

The product 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.

The event log should be readily retrievable for authorised personnel. The log could be stored separately from the product but in any case, should be secure.

For audit purposes and suspicious behaviour analysis, the logging of remote access activity should include user identification.

The size of the event log should be sufficient for the deployment context.

8.2. Updates

8.2.1. Security updates

To maintain or enhance cybersecurity of a product during its security update support period, it should have the ability for firmware or software to be upgraded or updated. This may be delivered locally or remotely.

8.2.2. Update validation

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

8.2.3. Roll-back

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

8.3. Priority

8.3.1. Normal operation

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

8.3.2. Local operation

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

8.3.3. Remote operation

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

8.4. Remote user authentication and access

8.4.1. Minimum privileges

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

8.4.2. Identification and authentication

Users accessing the system remotely should be uniquely identified and authenticated (e.g. using passwords, biometrics, certificates, etc.)

8.4.3. Usernames and passwords

Where usernames and passwords are used for remote user authentication, passwords should be in accordance with https://www.ncsc.gov.uk/cyberaware/home.

Note: *Usernames and passwords are not the only method of authentication.*

8.4.4. Additional authentication

Users remotely accessing the system should be required to provide at least one additional form of authentication over that used for local access, e.g. something they know, something they are or something they have.

Note: *Use of a PIN code alone is not sufficient.*

8.4.5. Session start

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

8.4.6. Credential input timeout

Incomplete credential inputs (e.g. login credentials entered but not submitted) should timeout and the input fields cleared.

8.4.7. Multiple session control

The same remote user identity should not be used for multiple concurrent remote sessions.

8.4.8. Loss of communications

Prolonged loss of communications during a remote session should automatically terminate the session.

8.4.9. Dormant session control

Dormant remote access activity for a prolonged period should automatically terminate the session.

8.5. Management of data integrity

Note: *Attention is drawn to Data Protection Legislation in relation to data security, transmission, storage and deletion.*

8.5.1. Data storage

Storage of data on a remote device should be encrypted e.g. data stored on a mobile phone.

8.5.2. Data transmission

Data transmitted across a remote connection should be encrypted.

Mechanisms should be in place to prevent replay attacks, or modification, or substitution of valid remote messages.

All data received via a remote connection should be checked for its integrity before use.

Note: *For example, using the mechanisms described in BS EN 50136-1:2012+A1:2018 Clause 6.8.1.*

8.5.3. Data removal

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

Note: *BS EN 50131-1 intruder alarm mandatory event logs are not considered as personal data.*

8.6. Product documentation

Documentation for the product should include the following information:

a) How to install, configure, commission and decommission a product securely.
b) Details of security impact for any configurable security option.
c) The security update methodology.
d) Where to obtain genuine software, and how to verify software is genuine.
e) Vulnerability disclosure mechanism, including the public point of contact for interested parties to report suspected or confirmed cybersecurity incidents.
f) How to use and operate the product securely.
g) A statement of the potential impact on operation of the product if security measures are breached e.g. access to sensitive data, sabotage and botnets (DDoS).
h) Details of any product certification, claims of compliance, test certificates and statutory requirements relating to the use of the product.

Note: *Documentation may be supplied in various formats, e.g. electronic or paper.*

Annex A: Sources of useful information – informative

A.1 Security design methodologies for products

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
11. ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements
12. BS EN IEC 62443 series of standards

A.2 Other

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

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 companies in the development of this code of practice:

Eaton
Horizon Two Six Ltd
Pyronix Ltd
Time and Data Systems International Limited

For other information please contact:

British Security Industry Association

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

BSIA Ltd
Anbrian House
1 The Tything
Worcester
WR1 1HD