National Cyber Security Centre
a part of GCHQ

Connected Places Cyber Security Principles

These principles will help ensure the security of your connected place and its underlying infrastructure, so that it is both resilient to cyber attack and easier to manage. The principles are grouped into three sections.

1. Understanding your connected place
2. Designing your connected place
3. Managing your connected place

1 Understanding your connected place

The first step is to develop understanding and context for your connected place.

What is a connected place?

A connected place can be described as a community that integrates information and communication technologies and IoT devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens.

1. Understanding your connected place and potential impacts

- Who has overall responsibility and accountability?
- What dependencies does your connected place have?
- What staff, expertise, infrastructure, and facilities are required?
- What will your IoT network look like and where will your sensors and IoT devices be placed?
- What data will be collected, processed, stored, and shared?
- How does your operational security work?

2. Understanding the risks, must include:

- the resilience your system requires
- the impacts to services in the event of performance degradation or failure
- the architecture (including users, devices, and services)
- the types of data you (or others) hold
- the connections you have (and how they are connected)
- the products and protocols needed to support authentication, authorisation, and protection
- the types of accesses required
- how policy enforcement points are implemented

3. Understanding governance and skills

- Ensure board level ownership.
- Make connected place business goals and priorities clear.
- Ensure decision makers have the right security, business and technical knowledge.
- Ensure responsibility and accountability for system security throughout the whole system life cycle.
- Provide staff with the right skills and opportunities.
- Build trust with your citizens to maximise engagement.

4. Understanding your suppliers' roles, including:

- how to communicate the minimum security requirements to your suppliers
- what assurance requirements need to be built into your supply chain
- the maturity of their security protections and staff security arrangements
- how your supply chain will continuously improve its security
- how any suspicious or malicious activity will be reported
- understanding their security approach to foreign influence
- how to safely transition to new suppliers

5. Understanding legal and regulatory requirements

- Ensure that the data architecture of your connected place fulfils the regulatory requirements set out in the GDPR and the Data Protection Act 2018.
- Consider additional requirements, such as Health & Safety and Network and Information Systems (NIS) Regulations 2018.

NCSC.GOV.UK @NCSC @CYBERHQ @CYBERHQ National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

Connected Places Cyber Security Principles

These principles will help ensure the security of your connected place and its underlying infrastructure, so that it is both resilient to cyber attack and easier to manage. The principles are grouped into three sections.

1. Understanding your connected place
2. Designing your connected place
3. Managing your connected place

2 Designing your connected place

Having developed understanding and context for your connected place, the priority should now be to make compromise difficult for any attacker.

6. Designing your architecture

- Understand the data that your system will ingest and its originating source.
- Consider which elements of your system need to have the highest levels of trust, and which would result in the biggest impact if compromised.
- Ensure that protections in place are appropriate for the services you are aiming to protect.
- Maintain appropriate trust levels in the tiers of your network most critical to your connected place.
- Identify any services or infrastructure that might bypass your controls.

7. Designing to reduce exposure:

- implement firewall rules which deny everything except for agreed critical network services
- remove default configurations for sensors
- switch off unused or unnecessary services and close network ports
- isolate network management interfaces and constrain who can connect to the system
- ensure all code is securely developed
- use software products that are well supported and regularly patched
- ensure software does not run using administrator rights and adopts 'least privilege' access

8. Designing to protect data - assurance of:

- what data is collected, stored, and where it may be accessed
- whether your data is stored or processed by a vendor or on a third party platform
- how your data is protected at rest and in transit
- the points at which data may converge within your connected place system
- your responsibilities in the result of a data breach

9. Designing to be resilient and scalable

- Ensure you can scale up the service (for example when demand increases) or when new services are added.
- Ensure the system is resilient to events, such as denial of service (DoS) attacks, component failures and administrative errors.
- Ensure the system degrades gracefully when limits are reached, rather than failing catastrophically.

10. Designing your monitoring

- The monitoring system needs to be independent from the operational connected place systems.
- You should include the visibility of interconnected systems, remote access into your system and connection attempts to internet systems from the network edge.

National Cyber Security Centre
a part of GCHQ

Connected Places Cyber Security Principles

These principles will help ensure the security of your connected place and its underlying infrastructure, so that it is both resilient to cyber attack and easier to manage. The principles are grouped into three sections.

1. Understanding your connected place
2. Designing your connected place
3. **Managing your connected place**

3 Managing your connected place

The priority should now be to manage your connected place's privileged accesses and supply chain throughout its life cycle.

11. Managing privileges

- Protect your management devices and network interfaces due to the privileged access they have.
- Only permit authorised devices to access your network management interfaces.
- Implement a robust user process that records joiners, leavers and movers.

12. Managing your supply chain

- Check the protections your supplier has in place to meet your security requirements.
- Ensure suppliers are actively monitoring the threat landscape.
- Ensure suppliers understands their role in mitigating identified risks.
- Ensure suppliers have documented how the system should be appropriately maintained and secured, once they have delivered against their contractual obligations.
- Ensure you have an incident management plan to help you manage incidents within your supply chain.

13. Managing your connected place throughout its life cycle

- Ensure there are clear responsibilities, processes, and procedures in place throughout the connected place's life cycle to assist those delivering evolving requirements.
- Decide how components are to be decommissioned at the end of their life, without increasing the risk to confidentiality, integrity, availability, and the quality of the service.
- Decide how components can be securely disposed of.

14. Managing incidents and planning your response and recovery

- Have a variety of methods for detecting incidents, including technical alerts from your monitoring, incident reporting and threat research from third parties such as partners and suppliers, and encouraging staff to report suspicious activity.
- Ensure you have incident management and response plans to effectively manage incidents to your connected place.
- Ensure incident response plans are tested or exercised.