

Secure Connected Places Playbook
Cyber security resources for local authorities



Department for
Science, Innovation,
& Technology

Supporting document for Connected Places Cyber
Security Principles 101

Presenter notes

This document contains presenter notes that can be used to support the delivery of the Connected Places Cyber Security Principles 101 presentation.



Slide 5 - What are connected places?

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101


What are connected places?

"The fundamental aim of a connected place is to enhance the quality of living for citizens through collaborative, interactive, and connected technology.

For the purpose of this guidance, 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.

A connected place will use a system of sensors, networks, and applications to collect data to improve its operation, including its transportation, buildings, utilities, environment, infrastructure, and public services."

- NCSC Connected Places Cyber Security Principles, May 2021



THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

5

Some examples of connected places technologies in local authority services are:

- **Traffic light management:** using sensors to optimise wait times and therefore pollution levels.
- **Waste management:** using sensors to improve the visibility of waste levels and oversight of suppliers, measuring their ability to meet their agreed service levels.
- **Streetlight management:** optimising power usage based on time of day, seasonality, activity and local crime data.
- **Parking management:** using sensors to provide smarter city navigation based on directing visitors to free parking spaces, thereby reducing emissions and congestion.
- **Environmental monitoring:** using sensors to monitor water levels in areas at risk of flooding, or air quality to provide citizens with clean air walking routes.
- **Social care, health and wellbeing:** the deployment of temperature and moisture sensors in houses to monitor and improve living conditions, or the use of sensors that help facilitate assisted living and improve accident response times.
- **Critical infrastructure and utilities:** crowd monitoring to determine town centre business and provide citizens with information on the best times to shop, or the use of smart local energy systems to reduce pressure on the grid.
- **CCTV:** for public safety and crowd monitoring.

These could use various networking technologies terrestrial (fibre), wireless (WiFi, Cellular LTE / 5G / NB-IoT, LoRaWAN) or satellite to communicate with fixed or mobile (drones, vehicles) assets.

Slide 6 - What is cyber security?

The slide is titled "What is cyber security?" and is part of the "Secure Connected Places Playbook" and "Connected Places Cyber Security Principles 101". It features a light blue background with a central graphic of a stylized building and a signal tower emitting concentric circles. The text is organized into three main sections: a definition, a quote from the NCSC, and a contextual explanation. At the bottom, there is a disclaimer and a page number.

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101

What is cyber security?

"Cyber security is the means by which individuals and organisations reduce the risk of becoming victims of cyber attack."

"Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data and devices."

- [NCSC What is cyber security](#)

In the context of connected places, cyber security is what makes connected places a safe place to live and to work. Designing connected places with an assumption that they will be compromised is a useful approach to ensure that appropriate controls are designed for detecting, protecting against, responding to and recovering from cyber incidents.

It is important to take a holistic approach when securing your connected places, considering personnel, physical and cyber security. Further information about personnel and physical security is available on the [CPNI website](#).

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

6

The NCSC defines cyber security as “the means by which individuals and organisations reduce the risk of becoming victims of cyber attack”.

In the context of connected places, cyber security is what makes a connected place a safe place to live and work. It is a crucial component to deploying new technology in public spaces and protecting citizens and infrastructure.

Designing a connected place with the assumption that it will be compromised is often a good approach to ensure that the appropriate cyber security steps are taken.

Whilst this presentation will focus on cyber security, it is also important to remember that a holistic approach to security is necessary, which should include personnel and physical security.

Slide 7 - What is the role of DSIT?

The slide features a light blue background with a graphic of a smartphone and signal waves on the left. The title 'What is the role of DSIT?' is centered in the upper left. The top left corner contains the text 'Secure Connected Places Playbook' and the top right corner contains 'Connected Places Cyber Security Principles 101'. The central text includes the Department for Science, Innovation, & Technology logo and name, followed by a paragraph about the National Cyber Strategy 2022, a paragraph about DSIT's role, and a paragraph about the Secure Connected Places team. A dark blue callout box on the right contains text about the Secure Connected Places Playbook. A footer at the bottom reads 'THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION' and the number '7' is in the bottom right corner.

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101

What is the role of DSIT?

 Department for Science, Innovation, & Technology

The [National Cyber Strategy 2022](#) outlined the Government's objective for the UK to be at the forefront of the secure and sustainable adoption of connected places technology.

DSIT's work contributes to this aim by delivering policy that supports the cyber security of the UK's connected places.

To do so, DSIT's [Secure Connected Places team](#) works closely with managers of connected places projects and suppliers of connected places technologies to ensure that communities across the UK can enjoy the benefits of secure connected places.

DSIT created the Secure Connected Places Playbook to complement the NCSC's Principles and support local authorities' connected place cyber security

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

7

DSIT's work contributes to the National Cyber Strategy which was published in 2022 and outlined the Government's objective for the UK to be at the forefront of the 'secure and sustainable adoption of connected places technology'.

In DSIT, this work is led by the Secure Connected Places team who created the Secure Connected Places Playbook to complement the NCSC Principles and support local authorities' connected place cyber security.

Slide 8 - Connected Places Threats

Secure Connected Places Playbook
Connected Places
Cyber Security Principles 101

Connected places threats

Cyber security
As places become more connected, and local authorities become more reliant on this connectedness to provide efficient services to their residents, the risk of hacking, malware, accidental misconfiguration and administrative abuse rises. Connected places are attractive targets to malicious actors as they process large amounts of data, and an attack on this infrastructure could have a societal-wide impact.



A traffic light prioritisation system that does not authenticate emergency vehicles would be open to anyone changing traffic signals to green, potentially risking lives and damage to vehicles.



In-home health monitoring can be abused for criminal and commercial gain. An attacker could target victims based on their activity patterns. Protecting individuals' privacy is vital.



Electric vehicle chargers should be protected. An attacker could sequence all chargers in the network to draw a large current simultaneously, causing a brownout (a drop in voltage in an electrical power supply system).

Privacy
As data collection is becoming more pervasive, the legal right to individual privacy needs to be protected. With such widespread data collection and correlation, seemingly anonymous datasets can be aggregated to deanonymise individuals.

Data privacy is a very important consideration when deploying smart infrastructure within connected places, particularly given suppliers may be exporting data outside of the UK as part of their service.

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

Connected places can be attractive targets to malicious actors due to the amount of data they process and the fact that an attack on this infrastructure could have a significant impact. As a connected place grows, and local authorities become more reliant on this connectedness, this risk increases.

Examples of the risks include:

- **A traffic light prioritisation system:** if it did not authenticate emergency vehicles, it would be open to anyone changing traffic signals to green, risking lives and damage to vehicles.
- **In-home health monitoring:** this could be abused for criminal and commercial gain and an attacker could target victims based on their activity patterns. Protecting individuals' privacy is vital, particularly where such sensitive personal information is involved.
- **Electric vehicle chargers:** an attacker could sequence all chargers in the network to draw a large current simultaneously, causing a brownout (a drop in voltage in an electrical power supply system).

It is also important to remember that as data collection becomes more pervasive, the right to individual privacy needs to be protected. With such widespread data collection and correlation, seemingly anonymous datasets can be aggregated and could identify individuals.

Slide 10 - Background

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101

Background

The National Cyber Security Centre (NCSC) released its Connected Places Cyber Security Principles in May 2021.

The Principles were developed in response to the increased use of smart and connected infrastructure being used to deliver public services in local authorities across the UK.

Whilst the adoption of connected places technology seemed to be increasing, there was a perception that security controls proportionate to the risk were not being considered.

It is principle-based guidance to support local authorities to make better-informed security decisions, not a baseline for compliance. The Principles were developed between the NCSC and a set of local authorities and industry.

[See the Principles in full here](#)

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

10

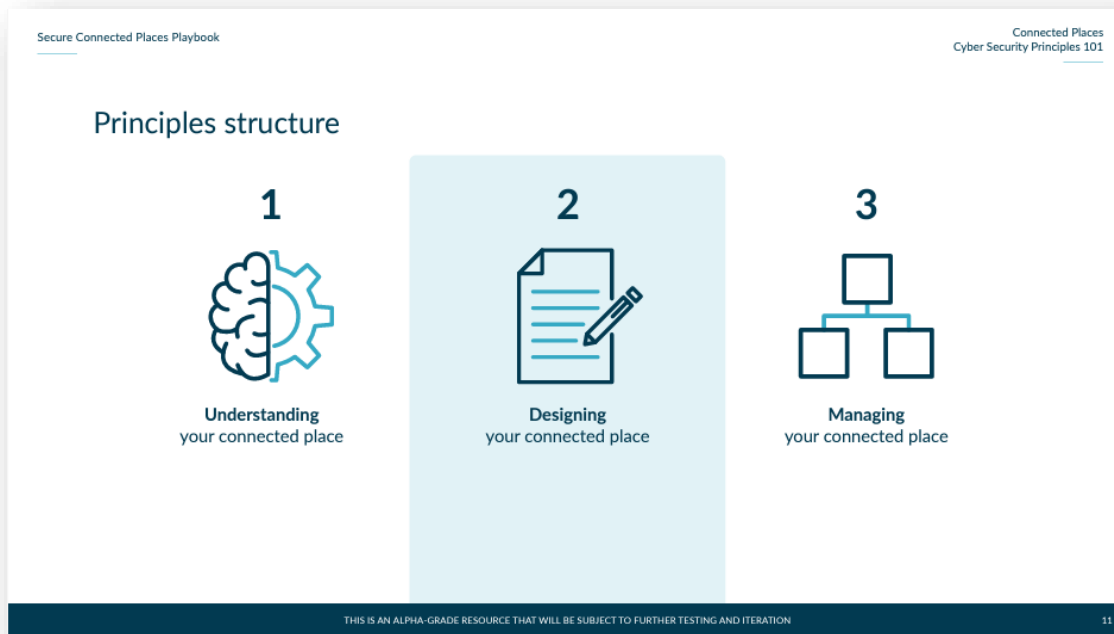
The National Cyber Security Centre published the Connected Places Cyber Security Principles in May 2021.

They were developed, in collaboration with local authorities and industry, in response to the increased use of smart and connected infrastructure by local authorities across the UK.

It is principle-based guidance to support local authorities to make better-informed security decisions rather than a baseline for compliance.

The following slides will provide an overview of the Principles.

Slide 11 - The Principles structure



The Principles are structured into three sections that relate to the phases of creating connected places. The first step in designing, building, and operating a connected place is to develop an understanding and context for it.

Having developed your understanding and the context for your connected place, the next priority should be to design your connected place in a way that makes it difficult for an attacker to compromise.

Then, having followed the connected place design principles, the priority should be to manage the connected place's privileged accesses and supply chain throughout its life cycle. This will include managing incidents, and planning for response and recovery. Importantly, this is not just for whole connected places, but should also be considered for each connected places project.

Slide 12 – Understanding your connected place

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101

Understanding your connected place

1. Understanding your connected place and the potential impacts
2. Understanding the risks to your connected place
3. Understanding cyber security governance and skills
4. Understanding your suppliers' role within your connected place
5. Understanding legal and regulatory requirements

It is essential to know your local authority's desired business outcomes and how these can be affected.

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

12

1. **Understanding your connected place and the potential impacts.** To identify what is critical to your connected place, a clear and complete understanding of its goals and ambitions is necessary.
2. **Understanding the risks to your connected place.** Knowing what assets and projects make up your connected place, as well as their dependencies and inter-dependencies is essential to know what risks exist. Knowing this, a risk management process can assess what risks are acceptable and require treatment. Understanding the risks is vital to knowing which business outcomes will be affected by any risk being realised. Please consult the Governance in a box resource for further details.
3. **Understanding cyber security governance and skills.** Having management ownership and a governance process for connected places enables alignment across the organisation and that training programmes are appropriately budgeted. Please consult the Governance in a box resource for further details.
4. **Understanding your suppliers' role within your connected place.** Connected Places can be complex systems with responsibility for service delivery split between the local authority and its suppliers. However, it is important to remember that whilst responsibility can be outsourced, accountability cannot, and therefore your local authority will remain the overall risk owner. Therefore, ensuring suppliers meet your requirements throughout a service's lifetime is essential. Please consult the Procurement and Supply Chain Management resource for more details.
5. **Understanding legal and regulatory requirements.** It is essential to understand the legal and regulatory framework within which your local authority must operate, this may vary based on the type of use cases being implemented. Statutory regulations, such as GDPR and the NIS Directive, must be observed regardless.

Slide 13 – Designing your connected place

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101

Designing your connected place

6. Designing your connected place architecture
7. Designing your connected place to reduce exposure
8. Designing your connected place to protect its data
9. Designing your connected place to be scalable and resilient
10. Designing your connected place monitoring

Building security in at the start of a project is widely considered more cost effective than having an attack and paying to remediate later.

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

13

6. **Designing your connected place architecture.** Understanding how your connected place is designed and architected is essential to assess whether it meets your organisation’s security requirements. For example, whether data is processed without first being validated and its sources authenticated. With an architecture understood, threats can be reasoned about, and decisions made as to whether residual risk within the systems needs to be mitigated by some means. Please consult the Threat Analysis resource for further details.
7. **Designing your connected place to reduce exposure.** Reducing the connected places attack surface (i.e. the interfaces of systems that are exposed to attack) will reduce the chance that an attacker will be able to successfully target your systems. System hardening e.g. closing down unused services and network segregation are good practice measures that can not only reduce the risk of an external attack but should the local authority become compromised can limit the blast damage.
8. **Designing your connected place to protect its data.** Connected Places by their nature collect and process data, it is therefore essential that it is appropriately protected. Personal information should only be collected if necessary and where it is, it is advised to protect it at rest and in transit. Maintaining a record of what data is collected, where and by whom it is stored and processed is essential not only for day-to-day operations but especially in the case of a security incident and potential data breach.
9. **Designing your connected place to be resilient and scalable.** Connected Places should be designed with the assumption that, at some point in their lifetime, they will be compromised, be it by an adversary or a mistaken user. To ensure resilience they therefore should be designed to be recovered easily and quickly. Connected Place projects often start as proofs of concepts, when they are determined to be business as usual they should be made scalable. This not only allows the local authority to flex its systems to its needs but also provides added resilience due to unexpected demand.

- 10. Designing your connected place monitoring.** A connected place's monitoring system should be out of the band to the connected place system itself. This approach ensures that a compromise of the connected place system can remain detected. Logging functionality of connected place technologies and supplier platforms should be utilised to identify incidents. The level of monitoring should also be commensurate with the criticality of the system, i.e. if a system is monitoring life-critical data, then its security monitoring should be frequent and rich enough to detect abnormalities rapidly.

Slide 14 – Managing your connected place

Secure Connected Places Playbook

Connected Places
Cyber Security Principles 101

Managing your connected place

11. Managing your connected place's privileges
12. Managing your connected place's supply chain
13. Managing your connected place throughout its life cycle
14. Managing incidents and planning your response and recovery

As your connected place grows – collecting more data and automating responses – it is likely to become of increasing interest to attackers and malicious actors. This increased automation and data sharing will also intensify the risk of cascade service failures across your connected place and its partners. Therefore, a mindset that assumes your connected place will be compromised is essential to being resilient and ensuring the continued provision of services.

THIS IS AN ALPHA-GRADE RESOURCE THAT WILL BE SUBJECT TO FURTHER TESTING AND ITERATION

14

11. **Managing your connected place's privileges.** Most systems provide different levels of accounts, devices and interfaces based on a particular user's rights within that system. Ensuring that those users that require increased levels of access are regularly reviewed and that they have secure means of accessing their accounts is necessary to maintain system security.
12. **Managing your connected place's supply chain.** It is important that if a supplier is providing you with services they adhere at least to your security requirements and that you maintain a right to audit their compliance with these requirements. Please consult the Procurement and Supply Chain Management resource for more details.
13. **Managing your connected place throughout its lifecycle.** Connected places each develop a life of their own. Understanding how the technology and its requirements change over that lifetime is essential to maintaining its security. Vulnerabilities will likely be discovered in technology utilised to build your connected place, therefore planning a vulnerability and threat management process that can manage and mitigate these is necessary. Devices and projects do at some point come to an end state, and understanding the security implications for how these are treated in their decommissioning ensures the security of any data is protected
14. **Managing incidents and planning your response and recovery.** "Inevitably security incidents will occur and in the context of connected places, this could result in degradation or loss of critical public services" – NCSC Connected Places Cyber Security Principles. Ensuring your local authority is monitoring for potential harm, that there are incident teams that can investigate attacks and playbooks for how the local authority may need to respond is advised in advance, doing so post-hoc can be extremely costly not only in monetary terms but also to the organisation's reputation.

Secure Connected Places Playbook
Cyber security resources for local authorities



Department for
Science, Innovation,
& Technology

Please contact secureconnectedplaces@dcms.gov.uk with any questions or feedback on these resources.

OGL

© Crown copyright 2023

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit
www.nationalarchives.gov.uk/doc/open-government-licence/
or write to the Information Policy Team, The National Archives, Kew,
London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk

This Playbook was produced in collaboration with:



plexal



DAINTTA



Configured
THINGS