National Cyber Security Centre
a part of GCHQ

Connected Places: Cyber Security Principles

Secure design, build and management of public realm technology, infrastructure, and data-rich environments for local authorities.

Contents

Introduction

This guidance will help authorities build awareness and understanding of the security considerations needed to design, build, and manage their connected places (often referred to as smart cities).

More specifically, it recommends a set of cyber security principles that will help ensure the security of a connected place and its underlying infrastructure, so that it is both more resilient to cyber attack and easier to manage.

This guidance is primarily for UK local and national authorities responsible for the design, build, and operation of UK connected places. It is particularly relevant for risk owners, CISOs, cyber security architects and engineers, and other personnel who will be running the day-to-day operations of the connected places infrastructure.

Note: Within this document, the terms connected place, public realm technology and data-rich environments cover the wider connected infrastructure, including local areas where data is collected through sensors and Internet of Things (IoT) devices. Within these connected areas, this guidance supports singular or multiple service functions. Such examples could include:

- traffic light management
- CCTV
- waste management
- streetlight management
- parking management
- transport services
- public services (such as health/social care, or emergency services)

What is a connected place?

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.

The challenges

A connected place provides a range of critical functions and services to its citizens. The systems that these functions and services rely on will be moving, processing, and storing sensitive data, as well as controlling critical operational technology. Unfortunately, this makes these systems an attractive target for a range of threat actors. A connected place will be an evolving ecosystem, comprising a range of systems that exchange data, which will only add further risks.

If connected systems are compromised, the consequences could impact the local citizens. Impacts could range from breaches of privacy to the disruption or failure of critical functions. This could mean destructive impacts, which in some cases could endanger the local citizens. There could also be impacts to the local authorities that are attacked. These could include a loss of reputation that could affect citizen participation, or the financial impacts of dealing with the aftereffects of an attack.

With this in mind, the NCSC has developed a set of cyber security principles to guide you in designing, building, and operating your connected place's systems securely. These should be read in conjunction with advice from the Centre of Protection of National Infrastructure (CPNI), focusing on physical and personnel security with a Security Minded approach.

Engagement with other stakeholders

As the national technical authority for cyber security, the NCSC's focus includes providing guidance designed to allow local authorities to better understand and manage the totality of their connected places ecosystems and technologies. The NCSC is prioritising engagement with local authorities, wider HMG, industry, and academia to ensure the cyber resilience of UK connected infrastructure. This includes:

- providing assurance for citizen privacy, through analysing and managing the threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of citizen data
- enhancing the wider cyber resilience of UK connected places in order to protect the services they provide
- working with our partners (including CPNI) to help support central government, local and regional authorities to secure the UK's connected places

System design

These connected place principles have been designed to be applicable to both digital systems and cyber-physical systems.

Throughout this guidance, we use the term system, by which we mean 'a collection of digital components that are connected using communication technologies to perform a business function.' A good example of this type of system is described in the NCSC's Operational Technology Design principles with Admin Corp. Admin Corp have to design and operate their systems to produce business assets, but must also protect these production mechanisms from cyber attacks.

We also use the term cyber-physical system, by which we mean 'a system that measures or controls the physical world to achieve a particular goal.' A good example is a smart traffic control system, which senses and measures the traffic patterns and conditions within a local area. The system can autonomously apply commands to the traffic signals to orchestrate and manage the movement of vehicles within that local area to meet prescribed objectives.

About the connected place principles

These principles will highlight key considerations that you need to keep in mind to ensure your connected place is designed, built, and operated in a secure manner. It is split into three sections:

- Understanding your connected place
- Designing your connected place
- Managing your connected place

These principles should be used in conjunction with existing NCSC and CPNI guidance. You should read, understand and implement the following:

- If your connected place is going to be built and operated within the cloud, refer to our Cloud security guidance and Virtualisation secure design principles.
- To help design your connected place system, refer to our Secure design principles and our white paper on Security architecture anti-patterns. You should also refer to our guidance on Systems administration architecture, Zero trust architecture design principles, Public Key Infrastructure principles and Secure communications principles (alpha release).
- To help manage your supply chain, please refer to our Supply chain principles.
- As a method of assessing the extent to which your organisation is managing cyber security risks in relation to your connected place's essential functions, refer to the Cyber Assessment Framework.
- For physical and personnel security principles (including security minded approaches) relevant guidance is available on the CPNI website. Examples include CPNI's guidance of Physical Security Systems, such as CCTV and access control.

.

.

Understanding your connected place

The first step in designing, building, and operating your connected place is to develop understanding and context for your connected place.

#1 Understanding your connected place and the potential impacts

The most important first step is to gain a clear and complete understanding of your connected place goals and ambitions. This will help determine which parts are critical and identify:

- Who has overall responsibility and accountability for your connected place?
- What dependencies does your connected place have (including dependencies on other systems or suppliers)?
- What is dependent on your connected place? What obligations do you have to the surrounding area or your citizens?
- What will your sensor and IoT network look like? Where will your sensors and IoT devices be placed?
- What data will be collected, processed, stored, and shared (such as information about citizens, area infrastructure, and key operational data)?
- What staff, expertise, infrastructure, and facilities are needed for your connected place to understand, design, and manage your connected place's operations effectively?
- How does your operational security work overall?

#2 Understanding the risks to your connected place

You need to have a clear understanding of your connected place infrastructure by identifying, understanding, and assessing inter-dependencies. This needs to include:

- Knowing your architecture, including your users, your devices, and your connected place services to manage your boundaries appropriately. Our Zero Trust Principles may be useful here in considering how to better understand and manage a connected places system, due to the ever-changing boundaries often inherent within connected places.
- The types of data you (or others) hold as part of the city infrastructure, to help determine your most critical areas.
- The connections you have (and how they are connected). Do they have a strong user and device identity, and do they authenticate everywhere?
- Have you determined what products and protocols may be needed for your components to support continuous authentication, authorisation, and the protection of your data in transit (moving from one connected component to another)?
- Who and how users have access to the system with controls in place. You will need to understand what types of accesses your business requires as part of your connected place operations. You will also need to determine where policy enforcement points are needed, to grant and deny access for connections to your connected place.
- The resilience your system requires, and the impacts to your services in the event of performance degradation or failure.

The risk owners within your connected place will need to determine what impacts they are **not** willing to accept within their connected place system. Examples could include events such as technology faults or cyber attacks that may cause traffic lights to change, thereby increasing the risk of car crashes, or databases of sensitive data being openly available to the public. The risk owners of the connected place should:

- work out what is most important to the operability of their services (this could be the data your connected data stores or transfers, or the underlying architecture it relies upon)
- understand and make some assumptions about the threats they may face
- identify vulnerabilities and threats that could exploit them within your connected place (for example by using threat modelling)
- use analysis to create a list of risks that you can prioritise according to how concerning they are

Risk decision makers could break the impacts down into sections to simplify analysis and decision making, for example using confidentiality, integrity, and availability for data risks. Here is an example of how these criteria might inform decision making. Similar analysis should take place to identify risks around hardware, software, and configuration.

Confidentiality: Only approved and specifically authorised personnel should be able to access connected place systems, and only to the extent necessary for their role. Any unauthorised access should be treated as a breach and any such breach could have consequences that may lead to the loss of privacy of citizen data. This itself could lead to a loss of trust, reputation, and may incur financial penalties for non-compliance in accordance with GDPR (and in extreme circumstances have national security implications).

Integrity: Your connected place derived data needs to be accurate, consistent, and used for its intended purpose. This requires strong non-repudiation and authenticity controls to stop data being modified or destroyed. Any such breach could have consequences that lead to a reduction in the effectiveness of the connected place operations. Additionally, consideration should be given to the integrity of data sources. Further consideration should be given to the characteristics of your connected place data sources, so they can be modelled for accuracy, completeness and validity to detect and alert to any suspicious readings and integrity breaches.

Availability: The connected place system needs to ensure timely and reliable access to (and use of) information. A breach could have consequences that could lead to the disruption of the day-to-day operations. For example, if the system were offline for more than half a day, it could create huge frustration for citizens unable to use services that are incorporated into the connected place (such as parking payments). Critical functions that rely on real time data should be capable of baseline functionality, even in the absence or loss of real time data.

For more information, please refer to the NCSC's guidance on Risk management.

#3 Understanding cyber security governance and skills

Your connected place cyber security needs to be owned, governed and promoted at the top level of the organisation that is responsible for the risk structure for both service resilience and user privacy. This accountability cannot be outsourced to suppliers. Essential tasks such as short and long-term planning need to be facilitated to support the local area and its citizens.

Over time, the services and functions of the connected place will become embedded within the everyday lives of its citizens. Therefore, you need to ensure that the connected place has the resources and funding available for its upkeep such as operational security, and improving future services in line with technological advances. This also needs to include security considerations behind the development, upgrading, and improvement of the technology to be able to deal with evolving threats and new capabilities. Tasks you need to think about incorporating into your governance process include investing in risk management and trusting your decision makers. As part of this, you should:

- make your connected place business goals and priorities clear
- identify assets that your connected place needs to achieve its business goals
- identify who within their organisation is responsible (and accountable) for the security of your connected systems
- identify who within their organisation is responsible (and accountable) for the ongoing security of your connected systems throughout the whole system life cycle
- understand and accept your connected place's inherent risks in delivering its services
- make sure the decision makers within your connected place have the right security, business and technical knowledge to enable them to make effective and timely risk management decisions

You also need to consider what skills and training is required. This needs to be incorporated into your planning for your connected place, which needs to include:

- Providing your staff with the right skills and opportunities to learn, so they can manage the security of your connected place effectively. This cannot be a single training opportunity where staff return to their daily roles once it has been completed. This needs to be an ongoing programme that aligns staff development with the evolution of your connected place and its surrounding technology. This will enable your staff to keep up to date with your connected place and be able to manage it more effectively.

- Building trust and being transparent with your citizens to maximise engagement with your connected place. This needs to include helping them to understand why there is a connected place, the role they have within it, and what data the connected place requires to function, whilst being transparent in providing assurance as to what data is being collected, and how you intend to use, store, and protect any data. This will help in building trust by clearly educating citizens, which will help encourage overall participation in the connected place.

For more information, please refer to the NCSC's guidance on Security Governance, enabling risk management decisions & communication.

#4 Understanding your suppliers' role within your connected place

You cannot outsource your accountability to your suppliers, as you are the overall risk owner for your connected place. There may be areas of split responsibility within your connected place that you may have with your suppliers, but it is still up to you to make sure the supplier fulfils this. You need to consider the role your suppliers have in building and operating your connected place. You should incorporate your suppliers' roles as part of your overall risk assessment process. This should include:

- What needs to be protected within your connected place, including systems assets and your citizens' privacy (and the level of protection required).
- How to communicate the minimum security requirements to your suppliers, how they will meet them, and what action will be taken in response to significant breaches of these requirements.
- Where operational technological capabilities are provided by the supplier to support bespoke business outcomes. This will bring bespoke risks with them which need to be analysed separately, as they will not fall within your minimum security requirements baselines. Further mitigations must also be implemented to deal with these bespoke risks.
- What assurance requirements need to be built into your connected place supply chain, and how these are going to be reported to you and your suppliers. Suppliers should be accountable for their security obligations as part of the contractual process.
- How your connected place supply chain is going to continuously improve its security, and build trust with your supplier.
- How your suppliers will report any suspicious or malicious activity, and assist you when needed.
- How readily you can change suppliers, should the need arise, and the level of support required to do so.
- What your exit strategy looks like (even if you hope not to use it).

Finally, you need to understand how you deal with risks associated with suppliers. This needs to include:

- Understanding the maturity of your suppliers security protections. Will these protections meet your security requirements that will make compromise difficult, and reduce the impact of compromise to the threats you may face?
- Understanding the maturity of your suppliers' people security arrangements. Are your suppliers' staff security educated to an acceptable level, with the awareness to spot suspicious activity, or potential physical or cyber attacks that you may face?
- Understanding the potential exploits and impacts that can occur from insider threats. Has your supplier performed risk assessments to understand their insider threat? Is there a plan to deal with insider risk ? Have they implemented effective controls to mitigate these insider risks? Have you considered implementing Privileged Access Management (PAM) to help support you?

Some countries seek to obtain sensitive commercial and personal data from overseas, including from the UK. They may also seek the potential to cause disruption to overseas services. Suppliers that are part of corporate groups based in these countries may be subject to influence from those governments to access and exfiltrate data from UK connected places, in support of those countries' security and intelligence services. Such suppliers may also be used as a vector for an attempt to take down an essential service through denial of service methods to affect its availability, or through poisoning of the service through data manipulation or malicious code injection that could affect the integrity and availability of the service.

Methods by which a foreign government may be able to influence a supplier include the following:

Ownership

Broadly, the greater the percentage of ownership of a supplier held by a foreign corporate group, the larger the influence that group will have on the affairs of the supplier. For example, for suppliers that are UK companies, a shareholding of 75% is required to pass certain important shareholder actions that require a 'special resolution' under the UK Companies Act 2006. The presence of intermediary companies in the chain of ownership between an overseas parent company and a supplier may dilute the extent of control.

Board representation

Foreign nationals on the board of a supplier may be directly subject to legal obligations in their country of citizenship to support that country's security and intelligence agencies, which they may feel pressure to comply with. It is important to note that these individuals will also be subject to countervailing obligations under UK law and/or the law of the supplier's place of incorporation (if it is not a UK company), for example data protection legislation.

Workforce

Foreign nationals in the workforce of a supplier may be directly subject to legal obligations in their country of citizenship to support that country's security and intelligence agencies, which they may feel pressure to comply with. It is important to note that these individuals will also be subject to countervailing obligations under UK law and/or the law of the supplier's place of incorporation (if it is not a UK company), for example data protection legislation.

Data hosting and routing

If UK connected place data is hosted in or routed through a foreign country, the government of that country may be able to influence the supplier to provide it with access to that data, or it may be able to access that data directly under national security and intelligence laws.

Supplier relationship

If the foreign corporate group is the manufacturer of products used by the supplier, that foreign corporate group will have influence over the supplier.

Provision of corporate services, knowledge or finance by corporate group

If a foreign corporate group provides corporate services to the supplier, the corporate group may be able to directly view or access certain data held by the supplier. The foreign corporate group may also provide knowledge to the supplier, which could be vital for that supplier's operations.

Investors

The same considerations outlined above with respect to suppliers also apply to the choice of investors in your connected places. You should consider the level of influence that a particular investor has over your connected places programme (including the ability to access and exfiltrate data or control essential services), and the risk that any investor may be subject to influence from a foreign government to act in a particular way.

#5 Understanding legal and regulatory requirements

You must ensure that the data architecture of your connected place infrastructure is built and configured to fulfil the regulatory requirements set out in the GDPR and the Data Protection Act 2018, including in your choice of organisations acting as data processors. Engage with the relevant bodies (including the Information Commissioner's Office) at the earliest opportunity to ensure legal compliance. You should also consider any additional legal and regulatory requirements that may currently influence your connected place, such as Health & Safety and Network and Information Systems (NIS) Regulations 2018. This is especially important if your connected place can affect safety-related or safety-critical systems. In addition, you should monitor future legal and regulatory requirements that may be relevant to your connected place.

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 connected place architecture

You need to ensure that your connected place architecture is designed securely. Your designs need to take into consideration the logical separation (or 'zones of trust') of your connected place network and identify critical security boundaries. This should not be limited to the cyber domain but also the cyber-physical (dual redundant sensors and/or actuators), and the physical space (such as diverse power supplies or communication routes). This ensures that if an incident occurs due to component failure or cyber attack, the impact is localised and failover options exist (as specified in the Design principles to make compromise and disruption more difficult).

You need to assess what protections are needed within your connected place. As with Principle 2, you need to understand and make assumptions about the threats your connected place may face, and analyse and deal with those top candidate threats. You then need to use methods such as threat modelling to identify how your connected place may be exploited (using STRIDE, for example). You will need to model your connected place by:

- Considering the importance of the services available, the operational data it relies on, and the privacy of citizen data that is held within your connected place. You then need to understand what the potential negative impacts may be if these were to be affected.
- Considering the internal or external events or attacks that may take place.
- Considering the threats and potential vulnerabilities over the horizon such as quantum computing.
- Considering each component within your connected place, how it protects itself from attack by making compromise harder, and how compromise is detected to be able to respond quicker.

For further information on threat modelling and determining security protections, here are some relevant blogs:

- NCSC Blog: NHS Test and Trace app security redux
- NCSC Blog: Securing the NCSC's web platform
- Microsoft Blog: Uncover Security Design Flaws Using The STRIDE Approach

When designing your connected place's architecture, considerations should include:

- Understanding of the data that your system will ingest and its originating source.
- Consideration of which elements of your system need to have the highest levels of trust.
- Consideration of which elements of your system would result in the biggest impact if compromised.
- Confidence that protections in place are appropriate for the services you are aiming to protect, and will detect or prevent an attacker from achieving their goals.
- Understanding of how data that services are responsible for are protected when at rest and in transit. You also need to implement protections from the data coming in from less trusted sources (such as the wider network and associated sensors).
- Ability for all connected place systems to validate, transform or render any external or low-trust data to neutralise potential incoming attacks.
- Maintaining appropriate trust levels in the tiers of your network most critical to your connected place.
- Identifying any services or infrastructure (such as management or monitoring) that might bypass your controls.

You also need to implement products, protocols and algorithms to enable authentication, authorisation, and the protection of your data in transit. Where practical, you should look to implement:

- the latest versions of products to close vulnerabilities before attackers can exploit them
- products that will give you the right level of confidence of their security ability (and have the latest version of these products)

- operational technology products and components supported by vulnerability management processes including consistent patching cycles
- the latest versions of secure protocols, deployed correctly so your data is encrypted to stop attackers being able to view and manipulate it
- strong cryptographic algorithms that provide you the right level of protection required

The NCSC has published guidance which can help with secure design:

- Design principles and operational technology guidance
- Pattern: Safely Importing Data
- Security architecture anti-patterns white paper
- Cloud security guidance: having confidence in cyber security

#7 Designing your connected place to reduce exposure

You need to ensure your connected place interfaces are only exposed where necessary, to reduce the attack surface. This needs to include:

- implementing firewall rules which deny everything except for agreed critical network services where appropriate (especially where services communicate with each other)
- removing default configurations for sensors and other information gathering systems (such as default passwords)
- switching off unused or unnecessary services and closing ports
- isolating management interfaces, and constraining who can connect to the system (and from where)
- integrating products that are well supported and have the right security characteristics you require within your connected place to give you confidence
- ensuring all code is securely developed (whether this is in house or from your suppliers); all software builds and pipelines need to be secured (regardless of who runs them), you can use our Defending software build pipelines from malicious attack guidance to support this
- where you are building and developing code yourselves, you need to design your code to restrict functionality to only allow those necessary for the service to operate
- using software products that are well supported including up-to-date and regularly patched software; do they have the right level of security that gives you confidence when used in your connected place?
- ensuring how and if the software protects your data in transit, protects your user accounts, and whether it provides logging and auditing
- ensuring all software does not run using administrator rights, and adopts 'least privilege' access control rights
- only allowing users limited data views of the system (and its data) by adopting access controls for 'least privilege' and on a 'need to know' basis by focusing on that user's job role
- controlling data behind demilitarized zones (DMZs) to stop an attacker from interacting with higher trust zones if it was compromised (where cross-border interactivity is unavoidable within your connected place architecture, strong authentication mechanisms need to be in place to control access to these areas that are exposed)

#8 Designing your connected place to protect its data

Connected places rely on the collection and processing of huge amounts of data. Taking a data-driven approach to governing and operating a connected place can bring significant benefits in terms of efficiency and improvements to the quality of life of citizens.

However, the storage and transportation of data are not without risk; where there is potentially sensitive bulk data there will be threat of attack or accident. Your connected place system design should not cache unnecessary data. These data stores are likely to be less well protected than the primary data store, but can potentially yield high-value or sensitive information to an attacker. Care should be taken to protect data at rest and in transit, with a primary focus on resilience of services and the privacy of the citizen.

You should make sure that you understand:

- what data is collected, and the benefits and risk associated with that data
- where your data is stored and where it may be accessed (all access should be authenticated, authorised, and logged)
- if your data is stored or processed by a vendor or on a third party platform
- what data is shared via your public APIs
- how your data is protected at rest and in transit (and be able to demonstrate it)
- the points at which data may converge or aggregate within your connected place system, and additional risk(s) to confidentiality or privacy that this may pose

You should also understand your responsibilities in the event of a data breach, and have procedures in place to handle such an event. This needs to include managing your data in high trust zones by moving it as far away as possible from the untrusted edge quickly. The Information Commissioners Office (ICO) and the NCSC have issued guidance on data protection that:

- outlines how to secure bulk personal data
- ensures you are acting in accordance with GDPR and that you can demonstrate compliance

#9 Designing your connected place to be resilient and scalable

Your connected place design needs to be able to scale up the service (for example when demand increases, or when new services are added). Planning for the future needs to be part of your connected place's design, to allow for your systems to be easily scaled, and resilient to attack.

Your connected place should be demonstrably resilient in the face of increased demand, denial of service attacks, or other events such as component failures through to administrative errors. Thought should be given to define acceptable levels of service when faced with increased demand, and the speed at which the system should scale to meet this. When limits are reached, the system should degrade gracefully, rather than fail catastrophically.

#10 Designing your connected place monitoring

Your connected place monitoring system needs to be independent from the operational connected place systems. This ensures that if the system operating the connected place is compromised, the attacker will have no visibility of whether the breach has been detected, and cannot remove their tracks from the logs.

Your monitoring design should give you visibility of all aspects of your connected place system, including endpoints and network edge devices. You should look to understand and create a baseline view of the normal operations of your connected place, which will enable the detection of abnormalities, and help you be better placed to identify true and false events. As threats and technology evolve, so must your monitoring and event selection, which will enable wider visibility of your system. You can use threat hunting exercises and tools to support this, such as the MITRE Attack Framework. Taking these steps will assist your ability in being able to monitor the areas of your connected place that rely on key data inputs and outputs.

Before designing your monitoring system, it is important to understand the context of your connected place operations first. This will enable you to develop and capture requirements that need to be considered and developed into the design of the system. Within your monitoring design, you should include the visibility of:

- interconnected systems, sources, and cross-service areas
- remote access into your system (including service or maintenance access by employees and third party suppliers)
- connection attempts to internet systems from the network edge

Depending on your connected place, this could include data from traffic lights, streetlights, CCTV systems, parking sensors, pollution sensors, noise sensors, and other IoT devices that are part of your connected place infrastructure where these components produce security events or logs.

For more information, please refer to the NCSC's blog on What exactly should we be logging?

.

Managing your connected place

Having followed the connected place design principles to make compromise difficult for any attacker, the priority should now be to manage your connected place's privileged accesses and supply chain throughout its life cycle. This will include managing incidents, and planning your response and recovery.

#11 Managing your connected place's privileges

Within your connected place, there will be areas of your system that will have the means to perform privileged activities that are not available to a standard user. You need to consider how you are going to manage these privileged accesses securely to reduce the risk of these areas being compromised, as this could lead to an attacker gaining unrestricted access to your system. This level of access may provide an attacker a platform to access sensitive data, such as operational or citizens' data, or be able to disable or degrade a critical aspect of your connected place. Considerations should be taken for the security of the following.

Management devices

You must protect your management devices due to the access they have. If an attacker compromises one of these devices, they could inherit the same level of privileges that the device has access to, which may include accounts and services that manage the connected place. It can be tempting to perform management from the same devices from which email and web browsing are typically conducted, but this should be avoided as it provides the attackers an easy opportunity to inherit privileges that could negatively impact your connected place.

Due to the risks and opportunities for exploitation from these devices (such as spear-phishing), and the massive impact of a compromised privileged account, it is imperative that management functions of a connected place are conducted on devices that are regarded to be at a high-level of trust. You should use a dedicated Privileged Access Workstation, or PAW, in cases where the impact is critically damaging. This provides the opportunity to add additional controls and measures that can be applied to reduce the attack surface.

Management interfaces

You must protect your management interfaces due to the access they have. If an attacker compromises one of these interfaces, they could inherit the same level of privileges that the interface has access to, which may include accounts and services that manage the connected place. If the interface is exposed, attackers may try and brute force the password or use an exploit to gain access.

You should manage these risks based on where your interface is located, what can access it, and who the users are that need access to it. Users requiring access to your management interface need to be authenticated, and where possible, multi-factor authentication (MFA) should be enabled. Only permit authorised devices to access your management interfaces, use PAM and implement principles such as 'just in time' and 'just enough' privileged access.

Privileged accounts

You must carefully manage the accesses privileged accounts have. If an attacker compromises an account with privileged access as mentioned in any of the attack types above, they could misuse the privileges they have access to, such as reading citizen information or making unauthorised changes that could affect a service within your connected place. You need to determine what rights and privileges users need to perform their roles and implement the principal of least privilege. You need a robust joiners, movers, and leavers process for users, so they do not inherit privileges they do not need.

For more information, please refer to the NCSC's guidance on Secure system administration and Protecting system administration with PAM.

#12 Managing your connected place's supply chain

Supply chain controls need to instil confidence and trust to ensure your connected place has the right levels of protection. This needs to be effectively managed by the supplier to reduce the risk to systems and data under their control. You should encourage your supply chain to consistently improve its security hygiene (alongside your security requirements) to deal with the same sort of threats that constantly lead to issues such as malware or ransomware.

To do this, you need to make sure:

- You have clarified with your supplier what level of security is required for your connected place. You can do this by establishing a minimum set of cyber security and functionality expectations and hold your suppliers to account contractually.
- You have the mechanisms to check that the protections your supplier has in place meet the level of security required for your connected place. You should implement the 'right to audit' into all contracts and exercise this.
- Your supplier is actively monitoring the threat landscape and adjusting the protections that they have in place to deal with these threats.
- You have identified risks, and your supplier has a part in mitigating them. You need to specify these risks and hold your supplier to account contractually.
- Your supplier actively identifies potential risks and assesses their security performance within your supply chain. Where the level of security falls below the level of security required for your connected place, they need to provide upward reporting to you immediately, so you can proactively manage them.
- Your supplier supports your connected place throughout its lifetime.
- Where you identify suspicious events within your supply chain, you need to have an incident management and response plan to help you manage these incidents quickly and effectively.

For more information, please refer to the NCSC's guidance on Supply Chain Security.

#13 Managing your connected place throughout its life cycle

Throughout your connected place system's life cycle, its security and technology requirements will evolve. This requires a sustainable engineering approach to continuously develop its underpinning infrastructure for security purposes. There should also be consideration of any evolving interoperability requirements to enable continued development of the connected place's services. This needs to include maintaining your operational security by fixing bugs or dealing with functionality issues as technology evolves. Alongside this, assets need to be reviewed and monitored constantly, which will help to identify end of life/legacy components.

This needs to include:

- how components are to be decommissioned and replaced by new technology without increasing the risk to confidentiality, integrity, availability, and the quality of the service that the connected place provides
- how components can be securely disposed of so not to expose any sensitive data if the hardware was recovered
- ensuring there are clear responsibilities, processes, and procedures in place throughout the connected place’s life cycle to assist stakeholders, vendors and integrators in delivering these evolving requirements

You need to understand the impact of the components to your connected place, and that you have effective assurance in place that components are still meeting the required security levels needed to protect the system. You can do this by testing your system throughout its life cycle. This can be done through health checks, penetration testing, and continual review of risks and procedures. If you identify that the level of security has dropped below the required levels, appropriate mitigations need to be in place to reduce any risks in the short term. For the long-term support of the connected place system, you should be making arrangements to replace these legacy components as soon as possible.

#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. It is therefore essential that thought is given to your incident management policies and procedures, and that you plan for recovery in the event of an incident effecting critical functions or services. Following on from Principle 10, you need to have a wide variety of methods for detecting incidents. This could include:

- technical alerts from your monitoring architecture (such as connection attempts into your sensor zones)
- encouraging staff to report suspicious activity (such as phishing emails or social engineering attempts)
- third parties such as partners, suppliers, private companies or the public performing incident investigations and threat research

To effectively manage incidents to your connected place, you need to be well prepared; you may experience a security incident sometime in the future. To do this, you need an incident management plan that will oversee the incident, communicate with necessary parties, engage support (such as the NCSC incident management service), report discoveries of the incident to the necessary parties, and notify them throughout an incident. Effective incident management will pull the whole response together, including dealing with any communications, media handling, escalations, and any reporting issues.

You should follow the NCSC's Incident Management guidance to help develop your connected place incident management and response plans. This includes:

- Planning your cyber incident response processes
- Building a cyber security incident response team (CSIRT). Where you do not have the capability in house to cover all aspects of the response, we recommend you choose a CIR Product from the NCSC's Certified Cyber Incident Response Scheme
- Developing technical response capabilities
- Maintaining the building and upkeep of your capability

National Cyber Security Centre

a part of GCHQ

Crown copyright 2021

Photographs produced by permission from third parties.