

Tech guide

Smart building
cybersecurity



SmartScore



This guide demystifies smart building cybersecurity and provides a reference on how to achieve the requirements for the TF5: Cybersecurity category of the SmartScore certification.

As part of the certification process, we verify that you have an active approach to your building cybersecurity resilience rather than auditing the content of your policy or guaranteeing you against hacking.

It is designed for use by landlords and developers as part of their due diligence process on their cybersecurity journey and understand how to provide evidence to achieve credits within SmartScore certification.

Expected takeaways

1. What a smart building cybersecurity policy is and why it is important
2. Key steps and considerations for a smart building cybersecurity policy
3. How your cybersecurity policy can serve as evidence for your SmartScore certification



Why is smart building cybersecurity important?

Why care about smart building cybersecurity?

Smart Buildings have more interconnected Operational Technology (OT) systems and Internet of Things (IoT) devices than traditional buildings. The potential for cyber risks is increased. The greater the connectivity and automation ecosystem, the wider the potential attack surface and vulnerability exposure to threat actors. Therefore, it is important to consider cybersecurity as a key factor of your building design and operations.

A strong cybersecurity approach is essential in preventing attacks that aim to access, alter, or delete organizational or user data as well as disable or disrupt systems or devices operations.

What is a smart building cybersecurity policy?

A smart building cybersecurity policy ensures the security of the Operational Technology (OT) systems and Internet of Things (IoT) devices in a building is maintained by securing:

- The cybersecurity built-in OT and IoT technologies
- Implementation of the technology by integrators.
- Ongoing operation of the technology

As such, it expands focus from typical IT systems to include the security of all of the individual building systems and devices, their interconnectivity and their access to/via the web which are intrinsic factors in smart buildings.

Typical steps on your cybersecurity journey

1.

Finding an expert

Find a cybersecurity expert versed in OT and IoT systems that could help your IT, OT & IoT systems and architecture to assess your building cybersecurity ecosystem and develop and implement your cybersecurity program.

2.

Internal assessment

Engage with your internal stakeholders to discuss and assess your current cybersecurity needs, risk areas specific to your building and teams, and highlight any historic or reoccurring threat events. Appoint an internal cybersecurity champion.

3.

Draft your strategy and policy

Create or update your cybersecurity strategy. The cybersecurity policy, implementation and assessment plans are key components of the overall strategy. The strategy and policy are ever-evolving documents adaptable to the changing threat landscape.

4.

Leadership onboarding

Seek support and buy-in from your leadership team to encourage transparency, alignment and funding for a cybersecurity program across the entire building ecosystem.

5.

Network discovery

Carry out an asset discovery and network mapping to understand your current risk. Identify all existing internal and third party assets connected to the network such as BMS, lifts, IoT devices and sensors, cameras, etc. Ensure you've started with your critical assets and included solutions managed by external supplies.

6.

Exposure reduction

Action with your internal team any immediate risk reduction measures such as the patching of devices where possible (eg. printers), segmentation of IoT devices across VLANs and enablement of active monitoring.



Key considerations

These impact the cyber resilience of a smart building and should be considered during the implementation of your cybersecurity policy.

Further detail is given on the following pages.



OT/IoT vs IT
cybersecurity



Logical level network
segmentation



Supply chain
management



Stakeholder
buy-in



Internal
cybersecurity
awareness

OT/IoT vs IT cybersecurity

Smart building cybersecurity goes beyond a corporate IT policy and extends into OT and IoT systems where cyber attacks manifest differently. Having a great IT cybersecurity regime does not mean you will be secure against OT/IoT-related threats: IT cybersecurity solutions do not usually work in OT/IoT environments and can even cause failure and malfunction.

Typical stakeholders:
IT / FM / security

Recommendations:
Be clear about roles and responsibilities.

Ensure you have an in-house OT/IoT cybersecurity champion.

Have an up-to-date inventory of all systems devices on the OT/IoT network and track which version of the software is installed.

Monitor all device activities to be made aware of any suspicious activity.

Quick glossary for this section:

IT
Information Technology refers to the critical infrastructure required for data processing. IT systems serve as repositories for corporate information.

OT
Operational Technology relates to building systems and controls such as HVAC, cameras, access control, etc. OT systems monitor events, processes and devices, and make adjustments in operations.

IoT
Internet of Things refers to devices on the network that are connected to the internet, communicate with each other and provide real-time data such as smartphones, wearables, smart meters, sensing devices for occupancy, parking, etc.



Network segmentation at logical level

Having OT & IoT systems integrated into the same network infrastructure increases the risk of cyber threats across systems, but restructuring the network may be cumbersome and costly. Logical segmentation is a best practice where the IT, OT & IoT systems are kept in dedicated virtual networks running in parallel but still using the same physical infrastructure.

Typical stakeholders:

IT / FM / security

Recommendations:

Consider network segmentation for building systems as secondary networks with multiple VLANs and subnets, different firewalls and managed switches.

Monitor and control all inside and out touchpoints into siloed core building system networks.

Consider having an automated process in place to monitor and track network vulnerabilities.

Treat any suspected incidents as real until proven false and resolve in a timely manner.

Supply chain management

As many services and solutions are provided by external suppliers and are often managed remotely, it is easy to lose oversight of all areas that may be exposed to external unauthorized access. A single device with poor security on your network can compromise the security of the whole network, so being able to easily and reliably test and audit all new devices is critical.

Typical stakeholders:

IT / FM / security

Recommendations:

Prescreen solutions or services to ensure adequate built-in cybersecurity and compliance to standards.

Conduct device whitelisting and qualification.

Integrate your security requirements in the T&C agreements, including responsibilities and insurance covers.

Manage and control all device passwords and remote logins.

Control and restrict access to your wider network.

Have an up-to-date active directory to track who has access rights and password status.

Control device exposure on the internet.



Stakeholder buy-in

Competing organizational agendas usually lead to disjointed cybersecurity initiatives and separate funding pockets without a holistic overview of the cyber threats of the entire building ecosystem. Usually, the cost associated with dealing with a cyber threat event once occurred is considerably higher than implementing preventive measures. Therefore, a cohesive strategy to align leadership buy-in is needed.

Typical stakeholders:

Leadership / IT / FM / security

Recommendations:

Engage in frequent cybersecurity conversation within the leadership teams.

Conduct table-top exercises to strategize response plan.

Focus on outcomes and start with an end goal in mind (e.g. how to deal with a specific situation such as ransomware attacks).

Ensure there is funding available for the cybersecurity ecosystem.

Internal cybersecurity awareness

Maintaining constant cybersecurity awareness for all employees and contractors working in the building is key for your strategy to succeed and be effective. Unaware employees can unintentionally leave open doors for your systems to be hacked. It is important to create a cyber-aware culture to prevent malpractices.

Typical stakeholders:

Leadership / IT / FM / security

Recommendations:

Appoint an internal cybersecurity champion literate in both IT and FM-related systems to oversee cybersecurity throughout the building lifecycle.

Invest in continuous staff training and cyber awareness programs.

Create adequate training specific to employees responsible for managing and operating the building.

Provide clear guidance on who to contact with internal questions related to cyber issues.








To achieve a cybersecure smart building you should consider the cyber resilience of the typical technology layers that make up the OT and IoT systems in a smart building.

When you develop a cybersecurity approach, you will need to:

- Consider what building systems and layers are relevant to your specific building (systems mapping)
- Create governance around cybersecurity to ensure the individual systems (hardware/software) and the interconnectivity between them (landlord integration network) and externally (landlord internet connection) are secure
- Develop a cohesive cybersecurity ecosystem considering what's needed within each evidence group

Do remember the key considerations mentioned over the previous pages:

-  OT/IoT vs IT cybersecurity
-  Logical level network segmentation
-  Supply chain management
-  Stakeholder buy-in
-  Internal cybersecurity awareness

Evidence groups

1. Governance

Clear processes, documentation and responsibility around cybersecurity over the entire lifecycle of the building ecosystem.

2. Software systems of the building

Effective monitoring and protection at the delivery and application layers via firewalls, gateways and encryption to prevent risks inherent from user interaction and third party applications.

3. Landlord integration network

Appropriate network segmentation of device groups with appropriate routing such as VLAN and secure data integration.

4. Landlord internet connection

Dedicated security protocols to manage cloud, third party and remote connections as well as exposure of IP connected systems and devices to the public internet.

5. Building systems

Cybersecurity considerations for onboarding, commissioning and ongoing assessment of the individual building systems and IoT devices.

Systems mapping

Delivery

Tenant Portal	Operations Portal	Enterprise Portal	Digital signage	Kiosk	Room Controller
---------------	-------------------	-------------------	-----------------	-------	-----------------

Application

Visitor Management	Health & Wellbeing Analytics	Sustainability Analytics	Maintenance & Operations Analytics	Occupancy Analytics	Video Analytics	Content Management System
Access Control	Work Order Management	Feedback / Surveys	Wayfinding / RTLS	Amenity Booking	Asset Information Model	Document Management

Platform

Common Data Platform

Network

Wired	Wireless	Gateways
-------	----------	----------

Device

Parking	E-mobility Charging	HVAC	Shading	Lighting	Metering	Elevator	Access Hardware	Onsite Electrical Generation
Fire Alarm	Cameras	Air Quality Sensing	Environmental Sensing	Occupancy Sensing	Real Time Location Hardware	Leak / Vibration Sensing	Smart Lockers	Smart Waste Sensing



SmartScore criteria for cyber security.

SmartScore checks whether your building has a cybersecurity policy that complies to industry standards and covers your approach to cybersecurity governance, assessment and implementation of the relevant technology layers in a smart building, such as:

- Software systems.
- Building systems.
- Landlord's integration network
- Landlord internet connection

Your policy may cover some or most of the elements outlined in the next pages but it should be specific to the requirements and needs of your building.

Under SmartScore section TF5: Cybersecurity, we verify the presence of a building level cybersecurity approach rather than audit the content of your policy or provide a guarantee against hacking.

SmartScore category TF5: Cybersecurity is broken down into the following three criteria:

1. Cybersecurity policy
2. Cybersecurity policy implementation
3. Ongoing cybersecurity assessments

TF5:1

Cybersecurity policy

Areas to consider for the details of the policy:

Compliance

Define how the landlord team and supply chain partners should comply with key cybersecurity standards or certifications, built into their products, services, processes and core building technological layers.

Cybersecurity standards to consider include but are not limited to:

- IEC 62443, 13335, 15408, ISO 27001
- ANSI 99.00.01
- NIST IR 7176, SP 800
- EU-level (European NIS Directive)

Documentation

Integrate security requirements into terms & conditions and assess suppliers to find potential protection leaks.

Ensure clear contractual policies regarding cybersecurity, integrity for third party products and services, including device and data access.

Ensure insurance policies are in place to cover cybersecurity events.

Process

The policy should include the process for how the implementation of new smart functionality needs to take into account appropriate cybersecurity measures. Measures may include, but are not limited to:

Establish user access configuration and control

Establish the process to be followed by employees or contractors in the event of a cyber incident occurring

Give consideration to how any cybersecurity policy has been ratified through the compliance mechanism of the landlord

Software update and patching of systems and network equipment

Appropriate network segmentation of device groups with appropriate routing eg VLAN

All network switches are managed and unused ports locked down

Device ports locked to MAC address of connected device

Network antivirus solution deployed

TF5:2

Cybersecurity policy implementation

Overview

The implementation plan should include records, commissioning reports or specification on how the cybersecurity requirements, generally outlined in the cybersecurity policy of the following parts of the building are addressed:

Considerations

Internal and external cybersecurity awareness

Continuous training and awareness plans to safeguard against cyberattacks

Security strategy for device lifecycle from onboarding, monitoring, servicing, management, software update and decommissioning

Supply chain management process

Details of how the cybersecurity policy has been applied at a logical level on the landlord integration network from integrator or manufacturer

Consideration should be given for how technical standards or certifications are maintained in connection with the building systems e.g. via centralised document control system

Details, e.g. system vendor / integrator documentation, on how the cybersecurity policy has been applied to all building systems. Asset inventory specifications, fields and identifiers

TF5:3

Ongoing cybersecurity assessments

Overview

Ongoing testing and validation of the cybersecurity performance of the building not only ensures that the implementation of the cybersecurity policy is fit for purpose but also that the building is not at immediate risk of being compromised. Considerations for your cybersecurity assessment include, but are not limited to:

Considerations

Active cybersecurity testing such as penetration and vulnerability testing undertaken at the commissioning of new features as well as on an ongoing basis across the building systems and integration network at least on an annual frequency

Testing and validation processes in place

Vulnerability and incident handling plan to include version updates and patching of different systems

Risk-based asset management process to identify and manage the security risks of all externally sourced components

Scheduling of when cybersecurity assessments are undertaken across the smart systems of a building on a regular basis, along with previous reports of cybersecurity assessments that have occurred over the last 12 months

Where next?

We're here to help.
With any questions, just get in touch.