Five Practical Steps to Protect Your Smart Building

A field-tested checklist for property managers and construction leaders

Executive Summary

Smart buildings improve comfort and efficiency, but the same features can be misused to disrupt heat, lighting, elevators, and doors. This checklist translates security best practices into plain, actionable steps you can assign, track, and verify—without diving into technical jargon.

Who Is This For & Why Now

- Property managers, operations teams, and construction leaders responsible for building systems.
- Recent incidents show attackers can lock out controls or change settings for leverage; an operations problem, not just IT.
- Regulators and insurers increasingly expect basic controls: inventory, segmentation, strong sign-in, plans, and testing.

---

1) Inventory & Monitor Every System

You can’t protect what you don’t know exists. Build a living list of control equipment and who can access it.

- **Action items:** List HVAC, lighting, access control, elevators, cameras, and all remote access paths.
- **Owner actions:** Assign a single owner; require vendors to declare remote access and support accounts.
- **Quick checks:**

    - Remove unknown devices and unused remote access
    - Document all panels and server rooms.
- **Metrics:**
    - % of systems inventoried
    - # of unknown remote connections closed

2) Segment & Secure the Control Network

Keep building controls on their own network, separate from office Wi-Fi and the public internet.

- **Action items:** Ensure building controls aren't reachable from the internet; separate from office networks.
- **Vendor access:** Use secure remote access with two-step sign-in; disable always-on open connections.
- **Physical:** Lock closets; disable live wall jacks or put them on an isolated guest network.
- **Metrics:**
    - # of control systems with internet exposure
    - # of vendor accounts using two-step sign-in

3) Harden Access: Remove Defaults & Use Two-Step Sign-In

Most breaches start with weak or shared passwords. Close this door first.

- **Action items:** Change all default passwords; give each person their own account.
- **Offboarding:** Remove vendor and ex-staff access when contracts end.
- **Two-step sign-in (MFA):** Require it for remote access and admin accounts.
- **Metrics:**
    - % of systems with unique credentials

    - % of admin accounts using two-step sign-in

4) Incident Playbook & Drills

Plan for a bad day so you can restore control fast—without panic.

- **Runbook:** Who decides to switch to manual? How to override doors, elevators, and HVAC safely?
- **Backups:** Keep controller configurations backed up offline; verify you can restore them.
- **Practice:** Run focused tabletop drills with facilities, security, and key vendors.
- **Metrics:** Time to restore to safe settings during a drill; # of configs backed up and tested.

5) Independent Security Checkups

Aim for **comprehensive checkups** led by an **independent expert** who assesses your **entire security posture** end-to-end (people, process, physical, and technology).

- **Scope:** Internet exposure; network separation; remote access paths; user accounts/offboarding; physical security of closets & ports; configuration backups/restore; change control; vendor access; incident playbooks & manual overrides.
- **Method:**
    - Onsite walk-through
    - Stakeholder interviews
    - Documentation review
    - **A non-disruptive** validation of controls.
- **Deliverables:**
    - Prioritized findings with risk/impact, practical fixes, named owners and due dates
    - A re-test plan and evidence (diagrams/screenshots)

- **Metrics:**
    - Critical gaps closed; days to remediation
    - % admin/vendor accounts with two-step sign-in
    - % systems with tested backups

Reach out to us at info@whitetuque.com to book a meeting.

WHITE
TUQUE