# THE ENTERPRISE IOT SECURITY CHECKLIST

The Internet of Things (IoT) has found its way into all aspects of our lives. In particular, “consumer-grade” IoT devices such as smart TVs, thermostats, smart speakers, fitness trackers and other devices are now used regularly in enterprises, either purchased by staff or brought in by employees.

- [ ] Update all passwords (local and remote, if different) to strong passwords and use multi-factor authentication where possible. Do not use products with hard-coded passwords. Closely govern permissions for devices, delegating access only when necessary.
- [ ] Research and carefully review the security characteristics and privacy policies of the controlling apps and backend services. Do not use devices that rely on apps or services with poor security and privacy.
- [ ] Just as in guest networks, place IoT devices on a separate, firewalled, monitored network. This allows you to restrict incoming traffic, prevent crossover to your core network and profile traffic to identify anomalies.
- [ ] Turn off any functionality that’s not needed. This includes cameras, microphones or even connectivity itself (e.g., if a smart TV is merely for display, not connectivity). It may also include physical blocking/covering of ports, cameras and microphones.
- [ ] Verify that physical access does not allow intrusion (e.g., by factory reset, easily accessible hardware port or default password).
- [ ] Don’t allow (or severely restrict) automatic connections via WiFi or other means. This could even go as far as network device isolation if a device only needs to talk to the local router. This helps prevent device infiltration
- [ ] If incoming traffic is not blocked, check for open software ports that may allow remote control and configure or restrict them as appropriate.
- [ ] Enable encryption whenever possible so that data is never transmitted “in the clear.” Consider buying only devices that support encryption. Otherwise, consider using a VPN or other means to limit data exposure.
- [ ] Keep firmware and software updated (via automatic updates or monthly checks). Do not use products that cannot be updated.
- [ ] Closely follow the lifecycle of the devices so that they can be removed from service when they are no longer updatable or

secure