COMMERCIAL PROPERTY

CYBER SECURITY CHECKLIST

Today, more and more commercial properties are adopting smart technologies to improve energy efficiency, monitor equipment, automate routine maintenance and collect data. Similarly, Space-as-a-Service tenants' demand access to the latest IT and telecommunications. Of course, more technology demands better safeguards against cyber-attacks. Property firms must also "take appropriate security measures" to meet data protection obligations. This handy checklist outlines 10 basic cyber security precautions every commercial property must take.

IT POLICY
Review & update IT policies regularly.

IT/computer use policies should be reviewed and updated at least once a year. All employees should receive IT policy training and regular refreshers.

ACCESS CONTROL
Implement effective user access controls.

To prevent misuse and unauthorised access to systems and data, user privileges should be restricted based on roles, responsibilities and seniority.

FIREWALL
Ensure your network firewall is properly configured.

A firewall restricts access between your computers and the outside world. A misconfigured firewall can give easy access to an attacker.

ANTI-VIRUS
Install anti-virus software & keep it updated.

Today's anti-virus is highly sophisticated software designed to identify and remove the widest possible range of threats.

OPERATING SYSTEM
Keep your Operating Systems up-to-date.

Obsolete Operating Systems such as Windows 7 no longer receive technical support, bug fixes, upgrades or security patches. An obsolete Operating System is extremely vulnerable to cyber-attack and non-compliant with data protection regulations.

PATCH MANAGEMENT
Patch software & network devices regularly.

Software makers routinely deliver patches to improve functionality and fix security issues. Unpatched software is extremely vulnerable to attack and exploitation.

STRONG PASSWORDS
Always use strong passwords: Over 10 characters with a combination of letters, numbers and special characters. Never use the same password twice. Never write it down or share it with others.

Passwords safeguard your company's systems and data from attack. The length and complexity of your passwords makes them more resistant to hacking.

PASSWORD MANAGER
Use a password manager & multi-factor authentication (MFA).

A password manager stores passwords in an encrypted format and provides secure access to all your passwords with a master password. Multi-factor authentication provides an additional layer of security to passwords.

BACKUP
Have a secure & reliable backup system.

Data backup systems are your company's life insurance policy. If your building burns down or you're the victim of a ransomware attack, a reliable backup system means you can quickly recover all your data and resume business.

SECURITY AWARENESS
Make security awareness training compulsory.

Nine out of ten successful cyber-attacks start with a phishing email. Training your staff to spot suspicious emails and other common threats is essential for good security.