DIGITAL SIGNAGE

Security Best Practices

Digital signage, an innovative communication tool increasingly integrated with broader networks, requires robust security measures to prevent unauthorised access, data breaches and other disruptive purposes such as content manipulation. Implementing these best practices will help protect your business from potential cyber attacks.

Deploy Content Management System

☑Define Review Process ☑Implement Publication Policy

☑Monitor Content Integrity

Implement System and Software Security

☑Formulate Patch Management Strategy ☑Install Anti-virus Software

☑Disable Unnecessary Software and Service

Implement Account Management

☑Change Default Credentials ☑Apply Principle of Least Privilege

☑Use Strong Passwords and Multi-factor Authentication(MFA)

Formulate Data Protection Strategies

☑Encrypt Data ☑Implement Backup and Recovery Policy

☑Remove Old or Unnecessary Data

Implement Network Security

☑Implement Network Access Control ☑Monitor Abnormal Network Traffic

☑Deploy Dedicated Wi-Fi and Encrypted Protocols

☑Conduct Vulnerability Scannings

Implement Physical Security

☑Restrict External Port Access ☑Disable Unnecessary Services

☑Disable Auto-Run and Auto-Play

More about IoT Security Guideline for Digital Signage, Please visit:

Digital Policy Office
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

HKCERT
Hong Kong Computer
Emergency Response Team
Coordination Centre

政府資助計劃
Government-funded programme