Accolade Group NW – IT Security, Device- Management and Internet- Usage Policy

1. Purpose

This policy sets out the mandatory security, device- management, and internet- usage requirements for all Accolade Group NW equipment. Its purpose is to protect organisational data, reduce cybersecurity risks, and ensure secure, consistent use of technology across the organisation.

2. Scope

This policy applies to:

- All employees, contractors, agency workers, and third- party partners.

- All company- owned laptops, desktop computers, mobile phones, tablets, and accessories.

- All software, internet browsers, and removable media used on company devices.

- All approved Bring Your Own Device (BYOD) arrangements as outlined in Section 8.

- All systems, networks, and cloud services used for company operations.

3. Secure Configuration Requirements

3.1 Device Access Security

- All devices must be secured with a PIN, password, or biometric authentication.

- Devices must automatically lock after a period of inactivity, as configured by IT/Admin.

- Users must not disable or weaken lock- screen security settings.

3.2 Auto- Run and Auto- Play

- Auto- Run and Auto- Play are disabled on all laptops and desktop computers.

- Users must not re- enable these features or modify related system settings.

3.3 Approved Internet Browsers

- Microsoft Edge, Google Chrome, and Safari (on Apple devices only) are the approved browsers.

- Browser security features such as automatic updates, safe- browsing, and phishing protection must remain enabled.

3.4 Approved and Licensed Applications Only

- Only approved, licensed, and legally compliant applications may be installed.

- Users must not install unapproved software, freeware, trialware, or applications from unverified sources.

- All unsupported browsers and applications must be uninstalled using the device's operating system.

- Users must seek advice from IT/Admin if unsure how to remove unsupported software.

- All installations must be authorised by IT/Admin.

- IT may remove unapproved software without notice.

4. Firewalls and Network Protection

4.1 Device Firewalls

- Windows Defender Firewall must be enabled at all times.

- Firewall updates must be installed within 14 days of release.

- Users must not disable, bypass, or alter firewall settings.

4.2 Boundary Firewalls

- Boundary firewalls are in place for the company's ISP and routers.

- IT/Admin will review firewall settings annually.

- If a firewall password breach is suspected, the password will be changed promptly.

5. Malware and Web Protection

5.1 Microsoft Defender

- All company- issued devices must have Microsoft Defender installed, active, and up to date.

- Users must not uninstall, disable, or tamper with Defender.

5.2 Web Protection

- Microsoft Defender must block access to malicious websites.

- Windows Defender settings must prevent connections to malicious websites over the internet.

- SmartScreen, network protection, and reputation- based blocking must remain enabled.

- Users must not disable or alter these protections.

6. Security Update Requirements

6.1 Mandatory Updates

- All software, operating systems, and firmware must be kept fully up to date.

- Automatic updates must be enabled on all devices.

- Security patches, critical fixes, and Microsoft Defender signature updates must be installed within 14 days of release.

- Devices outside the update window may be blocked from company systems until compliant.

7. User Access Control

7.1 Access Permissions

- Users must only have access to systems and data necessary for their role.

- Administrator access is restricted to authorised IT/Admin personnel only.

- Users must not attempt to elevate their privileges or bypass access controls.

8. Bring Your Own Device (BYOD)

8.1 Mobile Phones and Tablets

Personal devices may be used for emails, Lief, Roster Elf, and Microsoft 365 only if:

- The device make, model, and operating system are provided to IT/Admin.

- Microsoft Defender is installed and updated within 14 days of release.

- Firmware is updated within 14 days of release.

- The device automatically locks after a period of inactivity using a PIN, password, or biometric authentication.

Personal devices must not be used if:

- The manufacturer no longer provides firmware updates.

- The device is jailbroken or rooted.

8.2 Laptops

Personal laptops may be used only if:

- The make, model, and operating system are provided to IT/Admin.

- The device runs Windows 11 or higher.

- Microsoft Defender is installed and updated within 14 days of release.

- Firmware is updated within 14 days of release.

- The user does not have administrator access.

- The laptop automatically locks after a period of inactivity using a password or PIN.

9. Compliance and Enforcement

- Non- compliance may result in restricted system access, removal of device privileges, or disciplinary action.

- IT/Admin may audit devices at any time.

- Any suspected security breach must be reported immediately.