Cyber Security Policy

Our cyber security policy outlines the guidelines and measures in place at Digital Unite to preserve the security of our data, systems and technical platforms.

As an organisation that relies heavily on technology to collect, store and manage information, we recognise that this also introduces potential vulnerabilities. We therefore take a proactive approach to cyber security, combining secure systems, appropriate controls and responsible behaviour from all individuals who access our data and systems.

Digital Unite operates as a fully remote, bring-your-own-device (BYOD) organisation. As such, we rely on all users to follow good security practices in order to minimise risk and protect the organisation, our customers and our partners.

This policy is reviewed regularly and updated in line with changes to technology and risk.

Scope

This policy applies to all employees, contractors, volunteers and any individual who has permanent or temporary access to Digital Unite systems, platforms, data or devices.

Confidential data

Confidential data is highly valuable and must be protected at all times. This includes, but is not limited to:

- Customer, partner and staff data
- Financial and operational information
- Internal documents, plans and communications
- Platform, product and technical data

All individuals are responsible for ensuring that confidential data is handled appropriately, accessed only where necessary for their role, and not disclosed to unauthorised parties.

Protecting personal and company devices

When individuals use personal or company devices to access Digital Unite systems, they introduce potential security risks. It is therefore essential that all devices used for work purposes are appropriately secured.

All users are required to:

- Ensure that all devices are protected with a password, PIN or biometric security
- Keep devices physically secure and not leave them unattended in unsecured environments
- Install operating system and application updates as soon as they are available
- Use antivirus software and firewall protections where appropriate
- Access company systems only via secure and trusted networks

Devices must not be shared with others where this could result in unauthorised access to company systems or data.

Email security

Email remains one of the most common sources of cyber security threats, including phishing, malware and social engineering attacks.

To mitigate these risks, all users must:

- Exercise caution when receiving unexpected emails, particularly those containing links or attachments
- Verify the identity of the sender before taking action
- Avoid clicking on suspicious links or downloading unknown files
- Be alert to common phishing indicators such as urgency, unusual requests or inconsistencies in the message

If there is any doubt about the legitimacy of an email, it should not be engaged with and must be reported.

Password management

Strong password management is critical to protecting access to Digital Unite systems and data.

All users are required to:

- Use strong, unique passwords for all systems and services
- Avoid reusing passwords across multiple platforms
- Keep passwords confidential and not share them with others
- Use the approved password manager (Keeper) to securely store and manage credentials

Passwords should be changed immediately if there is any suspicion that they have been compromised.

Secure transfer of data

The transfer of data presents a significant security risk if not handled correctly.

All users must:

- Only transfer data where it is necessary for legitimate business purposes
- Use approved systems and platforms (such as SharePoint and Smartsheet) for sharing information
- Ensure that recipients are authorised and that the data being shared is appropriate
- Prefer secure links over email attachments where possible
- Avoid the use of removable media such as USB devices unless explicitly required and approved
- Never transfer sensitive data over public WiFi

Care should always be taken to ensure that data is shared securely and only with appropriate parties.

Access to company systems

Digital Unite operates a “least privilege” approach to access control. This means that users are granted access only to the systems and data required for their role.

In practice:

- Access must be requested and approved through appropriate channels
- Users must not attempt to bypass access controls
- Login credentials must not be shared or used by others

Individuals with responsibility for granting access must ensure that permissions are appropriate and regularly reviewed.

Additional security measures

To further reduce the likelihood of security breaches, all users are expected to:

- Lock their devices when not in use, including when working from home
- Report lost or stolen devices immediately
- Report any suspected security threats or weaknesses in company systems
- Avoid downloading unauthorised or suspicious software
- Avoid accessing unsafe or suspicious websites

These simple measures play an important role in maintaining overall security.

Remote working

As a fully remote organisation, all users are required to maintain secure working practices regardless of location.

This includes:

- Ensuring that devices and data are kept secure when working from home or in public places

- Avoiding access to sensitive systems over unsecured networks
- Taking care to prevent unauthorised individuals from viewing screens or overhearing confidential conversations

Remote working does not reduce security responsibilities, and all users must remain vigilant at all times.

Cloud services

Digital Unite uses a range of cloud-based services to operate the business and deliver its work.

Key platforms include:

- SharePoint
- Smartsheet
- Hosting and development platforms (Digital Ocean, Learning Pool)
- Office 365 Suite
- SurveyMonkey
- Canva

Any new systems or services must be approved before use to ensure they meet security requirements and can be properly managed.

Incident reporting

Prompt reporting of security incidents is critical to reducing potential impact.

All users must report any actual or suspected incident as soon as possible, including:

- Lost or stolen devices
- Suspected phishing emails or malicious activity
- Malware or virus infections
- Accidental data exposure

- Any suspected breach or vulnerability

Early reporting allows appropriate action to be taken quickly.

Security management

Digital Unite supports cyber security through a combination of technical controls and organisational practices, including:

- Secure configuration of systems and access controls
- Use of appropriate security tools and protections
- Ongoing awareness and guidance for users
- Investigation and management of security incidents

Take security seriously

Protecting data and systems is essential to maintaining trust with our customers, partners and stakeholders.

Cyber security is a shared responsibility. By following this policy and maintaining good practices, all users contribute to keeping Digital Unite secure.

Contact us

If you have any questions, please get in touch: du@digitalunite.com