Cyber Security and Bring Your Own Device (BYOD) Policy

Version: Cyber Security Policy v2023_v2.Docx
Last Reviewed: 3 July 2023
Next Review: 31 December 2023

Contents

1 Introduction

This Policy outlines the requirements for BYOD usage and establishes the steps that both users and IT Support should follow to initialize, support and remove devices from company access. These requirements must be followed as documented to protect company systems and data from unauthorized access or misuse. This policy describes the steps that the company, its employees and contractors will follow when connecting personal devices to organization systems and networks.

2 Scope

This policy covers all full-time and part-time employees, contract workers, consultants, temporary workers, and other personnel granted access to organizational systems, networks, software, and/or data.

Equipment covered by this policy includes (but is not limited to);

- Desktops, laptops, and tablet computers
- Smartphones (defined as any cellular telephone that connects to the internet via Wi-Fi or a mobile provider network)
- Flash, memory, and/or thumb drives
- External hard disks
- Wearable devices such as watches, VR headsets, and augmented reality glasses with Wi-Fi or Bluetooth

3 BYOD Policy

All users must understand that whenever a computer device is connected to the organization's network, systems, or computers, opportunities exist for:

- Introducing viruses, spyware, or other malware.
- Purposefully or inadvertently copying sensitive and/or proprietary organization information to unauthorized devices.
- Introducing a technical or network incompatibility to the organization that the user is not even aware of.
- Loss of data that may adversely affect the organization if it falls into the wrong hands.

As a result of any of these circumstances, a user connecting their own device to organization resources, systems, or networks could interrupt business operations, cause unplanned downtime for multiple users, and/or cause a data breach releasing organization, client, and/or partner data to unauthorized parties. In worst-case scenarios (and in events entirely realized at other organizations), civil and criminal penalties for the user and/or substantial costs and expenses to the organization could arise.

4 User Responsibilities for BYOD devices

Individual users are responsible for ensuring that:

- Acuity has been informed of any BYOD that will be used to connect to the organization's resources, systems, or networks
- Use of removable media – flash drives, external hard drives etc is not permitted under any circumstances.
- Only approved applications should be downloaded to BYOD from official app stores and devices won't be 'rooted' or 'jailbroken' to allow unsigned applications to be installed. Apple users must only download from the App store and Android users only from the Google Play store.
- The device is set to auto-update and has all critical and security patches installed.
- The device does not have a virus, spyware, or malware infection.
- The device is properly encrypted if the potential exists for the device to save, cache, or even temporarily store organization data.
- The device is properly protected against viruses, spyware, and other malware infections and that the system has properly licensed anti-malware software, when appropriate.
- The device has a firewall installed and rules configured to prevent unwanted incoming traffic.
- The device does not have any third-party software or applications that pose a threat to the systems and networks or that could introduce application incompatibilities (any such findings should be removed before proceeding).

- The device does not have a static IP address that could introduce network incompatibilities.

- The device includes password/biometric security measures that will automatically lock the device after one-minute period of inactivity.

- In the event that a user believes a personally owned or personally provided device that is authorized to connect to the organization's resources, systems, or networks might be infected with a virus, spyware infection, or other malware threat or might be somehow compromised, they must immediately notify the IT department in writing of the potential security risk.
- If a user loses or misplaces a personally owned or personally provided device that is authorized to connect to the organization's resources, systems, or networks, they must immediately notify the IT department in writing of the potential security risk.

5 Passwords

Access for Acuity employees and contractors to owned applications and systems is granted solely to conduct legitimate business on behalf of Acuity. Access to specific system functions and data resources is consistent with each user's scope of employment and/or job responsibilities. User accounts will remain active until a user's work status relationship either changes or terminates. External users can access specific functions as stipulated on user login setup, accounts will remain active until notification by the user/organisation to revoke access or a period of non-use (<specify time period>) is exceeded.

- Passwords must
  - be a minimum of 8 characters in length.
  - Contain at least one (1) character from three (3) of the following categories: Uppercase letter (A-Z) Lowercase letter (a-z) Digit (0-9) Special character (~`! @#$%^&*()+=_-{}[]\|:;”'?/<>,.)
  - Passwords should be a combination that cannot be easily guessed. Examples of passwords that are not acceptable include user ID, first or last name of user, family member, city, town, street, etc
  - Not re-use a previously used password

- Acuity will force password changes for staff or contractors if ever there is a suspicion of a data breach or password being compromised.

- MFA for all users is enforced to prevent access to user accounts/applications by unauthorized users.

- Password must be kept confidential

- Managers must authorize access, on a need-to-know basis, to information systems for activities within their area of responsibility and will ensure user accounts are removed if user's role either changes or terminates

- Alternate authentication technologies, e.g., biometrics or proximity cards, may be used in place of password protections.

- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.

- Access privileges will be reviewed prior to granting access based on factors including job role and function (role-based access) or the individual (user-based access).

- User IDs, passwords or email accounts are not to be transferred to another individual.

6 Device Management

To ensure all devices provided by Acuity are used to access the organisations resources are secure the following are applied;

- Devices have Bitlocker encryption installed

- Devices will be joined to Azure AD

- All local accounts and local admin accounts removed (with the exception of the sole admin account)

- Any employees with Microsoft 365 logins will have their rights limited to only the extent of their user role

- Devices will have Autorun disabled

- Adobe Flash and Adobe Air products are removed from all devices

- Windows update is set to automatic

- All devices will have Microsoft Office versions updated to Office 365

- All unnecessary default accounts must be removed or disabled before installing a system on the network.

- Laptops have a user account without admin privileges, and an admin account, which is only used by the 3rd party support staff to carry out support tasks such as software installation. The third party support firm procedure is that admin accounts are not used for browsing the web, downloads or email, and as soon as the support task is completed the technician will log out from the admin account.

- Changing of user accounts such as email addresses will only be carried out by IT Support (sole admin account) on authorisation by a Director.

- New devices or applications will have the default password changed to follow password guidelines. Where appropriate a second member of staff will ensure this by attempting to use the old password to access the device/firewall/application.

- If a user believes their password has been compromised, it must be changed immediately and reported to IT support. Password changes are recorded in a log and the administrator will check with the user that the old password no longer works. Both the change and the check must be recorded in spreadsheet. **Laptops_Telephone Numbers.xlsx**

- Admin access rights will be reviewed every three months by IT support in conjunction with the company Directors to ensure that the correct user rights are still in place and still relevant to the organisation.

- Admin accounts will not be used to access websites or to download email and any software download will be carried out as a standard user.

7 Lost or stolen devices

In the event that a device has been stolen;

- You must notify Acuity immediately.

- Admin will block that users access and force a logout of all devices.

- Admin will remove the device from Azure AD to stop any further logins.

- Avast software can be used where needed to force a restart, (in the case where a device has been stolen while open and logged in). When the restart is initiated, it will then enforce the Bitlocker encryption pin.

8 User Account Set up

- User accounts will only be set up by IT support (sole admin account) and only when authorised by a company Director.

- Users will need to set a password following the company password policy.

9 Leavers / Account Deletion

When a staff member leaves the organisation the user's password will be changed by administrator using the Microsoft 365 admin centre preventing access to applications and data. All data are retrieved from their accounts and laptop, following which the account is deleted.

This process is checked by the administrator to ensure that the user can no longer log in to any services from outside the organisation. Completion of the steps in the process is recorded in the spreadsheet. **Laptops_Telephone Numbers.xlsx**