TEG BYOD Security Policy

Document Information

Version Number	1.0
Last Update	15/01/2023
Author	Matthew Coutts
File Name	TEG BYOD Security Policy
Document Title	TEG BYOD Security Policy
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	15/01/2023	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	15/01/2023	15/01/2023	Matthew Coutts

1 - Audience

This Policy applies to all employees, including permanent and temporary staff, contractors, who utilise a physical or wireless connection to Company of TEG (Company) network infrastructure.

2 - Scope

This Policy applies to any 'bring your own device' (BYOD) or accompanying media that may be used to access the systems and data of the Company, whether it is used within or outside the standard working hours.

3 - Purpose

Employees increasingly prefer to use their own smartphones, tablets, and other devices to access information. Empowering them to do so supports greater mobility and flexibility.

The purpose of this Policy is to:

- allow the use of BYOD's for work purposes, and access Company systems and data when and where it is needed;
- ensure that Company systems and data are protected from unauthorised access, use or disclosure; and
- set out the terms of use for BYOD's, the Company's rights, and the responsibilities of the Company and BYOD owners.

This Policy should be read in conjunction with the Information Technology Acceptable Use Policy.

4 - Definitions

In the context of this document the following definitions apply:

Defined Term	Meaning
Application or App	Computer software designed to assist end users to carry out useful tasks. Examples of applications may include the Microsoft Office suite of products or smartphone applications such as Google Maps.
Bring Your Own Device (BYOD)	Any electronic device owned, leased, or operated by an employee, contractor or affiliate of the Company which can store data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers, and netbooks.
Data	Any and all information stored or processed through a BYOD. Company data refers to data owned, originating from, or processed by Company systems.
Jail Broken Device	A device that has been tampered with to permit full access to the operating system, allowing the download of additional applications, extensions and themes that are unavailable through official means.

Minimum requirements	The minimum hardware, software, and general operating requirements for a BYOD.
Mobile Device Management (MDM)	A solution which manages, supports, secures and monitors mobile devices.
Wipe / Wiping	A security feature that renders the data stored on a BYOD inaccessible. Wiping may be performed locally or remotely, via an MDM product, or by a system administrator.

5 - Terms of BYOD Use

This Policy must be reviewed before using a BYOD. Acceptance of the Information Technology Conditions of Use Policy also constitutes acceptance of the terms of this Policy and indicates agreement to the standard terms of use outlined in this Section.

Any BYOD must meet the minimum requirements set out in this Policy.

The responsibility to meet the minimum requirements set out in this Policy rests with the BYOD owner.

BYOD capabilities and profiles must match Company requirements as well as user requirements for work. For example, a tablet or smartphone might be suitable for information consumers, whilst a laptop or desktop profile would be a better match for information creators.

BYOD users agree to provide limited authority to the Company to allow for the protection of Company data on the BYOD. This authority remains in place from the time the device is registered until the time it is de-registered, and includes:

- permission to wipe the BYOD in the event of loss or disposal. This may include the wiping of personal data, address books, and e-mail depending on the data classification of Company information stored locally on the BYOD, and whether a MDM tool is used; and
- permission to directly and/or remotely change the security configurations of a BYOD. These changes include, but are not limited to:
    - refusing to register a BYOD that fails the BYOD minimum requirements set out in this Policy, or that currently has installed banned software.
    - configuring certain security settings.
    - preventing the user from changing certain security settings.
    - applying a login code with an acceptable level of complexity to enable secure access to the device;
    - automatically locking the device after an inactivity timeout period.
    - installing software and digital certificates necessary to maintain security.
    - encrypting data stored on the device.
    - automatically wiping either all data or all Company data after a specific number of failed login attempts; and

- should any configuration be removed that are required for proper and secure use of the device with Company systems, these may be re-applied or access to Company systems and data will be restricted if the configurations cannot be reinstated.

Users are responsible for ensuring that personal devices are adequately secured against loss or theft.

Users are responsible for replacing, maintaining, and arranging technical support for their BYOD. The Company will only provide best effort support for any applications that the Company has provided, and for network connection troubleshooting.

Access to Company systems and data is provided at the sole discretion of the Company and access may be revoked at any time and for any reason.

The Company is not responsible for any personal loss or damage suffered as the result of actions undertaken by the Company to protect Company data stored on a BYOD.

If a BYOD is lost or stolen, and it contains Company data, the loss or theft must be immediately reported to the IT Service Desk.

All Company data must be removed from the BYOD at the end of its use within the Company environment.

Users are responsible for ensuring that appropriate licensing exists for operating systems and applications running on a BYOD.

Users acknowledge and accept the Company's rights, and all other provisions and requirements set out in this Policy.

6 - The Company's rights

The Company's rights are:

- any Company data stored on a BYOD remains the sole property of the Company.
- the Company has a right to inspect Company data held on BYOD.
- the Company may remotely monitor a BYOD to ensure security and software configurations are maintained.
- the Company may enforce policies on a BYOD to ensure the security of Company data. This may include but is not limited to enforcing screen locks, pin codes and the ability to remotely wipe Company data.
- the Company may push and remove data to and from a BYOD to enhance its security or manageability through the use of MDM;
- the Company may request an inspection of a BYOD in the owner's presence prior to them leaving the Company to confirm there is no Company data stored on the BYOD; and
- the Company has a right to enforce any provision or requirement of this Policy.

7 - Requirements

Bring Your Own Device Minimum Requirements

The Company's minimum requirements for BYOD's are outlined in the following table:

Function	Minimum Requirement
Configuration Management	
Operating Systems	A BYOD must use a legitimate, up to date, and vendor-supported operating system. This excludes 'jail broken' devices.
Network authentication	Network authentication is subject to the Company's requirements, being 802.1x for wireless or wired connection, and authentication via an SSL VPN for remote access to the network.
Password protection / User authentication	A BYOD must support password, PIN, or biometric authentication.
Automated Cloud Backup	Automated cloud back up must be able to be disabled.
Automatic Device Lock	A BYOD must have an automatic lock enabled.
Device hygiene	A BYOD must have appropriate and up to date anti-virus installed.

BYOD Registration, Configuration and Management

Each BYOD will be automatically registered within the Company's Office 365 platform upon first connection to the exchange email service.

The Office 365 platform incorporates MDM capabilities which can enforce security configurations on a BYOD.

A limit may apply to the number of BYOD's that can be registered for a single person.

BYOD owners will not be prevented from installing software or applications on their BYOD. However, the Company may block access to Company ICT services if any software, applications, or data present a threat to the Company's ICT environment.

Device Usage and Support

The use of Company services are at the sole discretion and risk of the BYOD owner.

While the Company will take all reasonable efforts to ensure service is available, the Company does not guarantee that access will be available at all times.

The Company will not impose a charge on BYOD owners for registering BYOD on the Company network.

BYOD owners are responsible for supporting their own devices. The Company will only provide limited support for any applications the Company has provided.

The following table outlines responsibilities:

Support	Responsibility
Physical provisioning	BYOD owner
Replacement of defective / damaged BYOD	BYOD owner
Operating system support, including licensing	BYOD owner
Application support of BYOD, including licensing	BYOD owner
Company provided / supported mobile applications	IT Service Desk
Company provided / supported applications such as Microsoft 365	IT Service Desk
Backing up and restoring data and configuration settings	BYOD owner
Device connectivity / access	**Responsibility**
Mobile internet	BYOD owner
Home internet / broadband	BYOD owner
VPN client	IT Service Desk
Company wireless	IT Service Desk
Minimum requirements	**Responsibility**
Meeting the minimum requirements outlined in this Policy	BYOD Owner

The Company is not responsible for:

- any costs incurred through BYOD use. The Company will not reimburse costs incurred by a BYOD owner or user in association with BYOD use, including but not limited to:
    - voice or data charges.
    - software or application acquisition fees.
    - support or insurance costs.
- any inconvenience that may be experienced in connection with using Company ICT services on a BYOD.

The Company will not monitor:

- the phone call or text message history of a BYOD. Where needed (for example, in the case of a disciplinary matter) the call and text messages may be requested;
- the web browser history on a BYOD when not connected to Company network(s), unless the web traffic is directed through the Company's network infrastructure.

The Company may:

- restrict access to internet websites or network services for operational or policy reasons while a device is connected to Company networks, including either wireless or cabled connections;
- collect information while monitoring the use of a BYOD while it is connected to the Company network.
- wipe Company data from a device in accordance with the following circumstances:
    - a BYOD is reported as being lost/stolen to the IT Service Desk;
    - the BYOD owner ceases employment or affiliation with the Company.
    - there is a suspected security breach for example but not limited to, modification of the BYOD's operating system, breaching Company policies, or the detection of viruses or malware on the BYOD.
- wipe personal data if it is stored with Company data within Company supplied applications in the circumstances listed in the clause above.

Protection of Company data on your BYOD

Company data classified as Highly Restricted or that is subject to legal or professional privilege must not be stored on a BYOD.

The Company may reset a password or access code, only in consultation with the BYOD owner.

Company data must only be backed up to approved locations within Company systems.

BYOD owners should check their BYOD to ensure that automated cloud backup is disabled to ensure that Company data is not inadvertently leaked, compromised or mishandled.

Users should take reasonable steps to reduce the risk of losing personal data. For example, storing personal data separately from Company data through file partitions or using a separate memory card.

Device De-registration

The Company at its own discretion, may:

- de-register any BYOD at any time without warning; or
- de-register a BYOD that has not consumed Company ICT services for more than 12 months.

BYOD Owners can de-register BYOD at any time by visiting the Office 365 portal. The BYOD may not be able to connect to Company ICT systems and data, unless it is re-registered.