Student ID 5472837
ZZCA9221 2023

Bring Your Own Mobile Device (BYOD) - Policy | Valeur Technologies Australia

CYBER MANAGEMENT AND GOVERNANCE (H523 ONLINE)

BASHIR, UMER

Valeur Technologies Bring Your Own Mobile Device (BYOD) - Policy

Valuer Technologies may grant individuals the privilege to access company data via personally owned devices ("Devices"). This privilege is contingent upon compliance with all company policies, applicable laws, regulations, and ethical standards. Individuals accessing company data must understand and adhere to the terms outlined in this policy.

1. **Accessing Company Data Privilege.** Company may allow You to access Company data (including email, documents, tools, applications, Teams, SharePoint, and other Microsoft services) ("**Company Data**") through your personally owned device ("**Device**") provided You use them in accordance with all Company policies and applicable laws, regulations and the like. Company may terminate Your authorization at any time, with or without notification, and You agree, as instructed by Company, to return or destroy (and provide written certification) any or all Company Data at the Company's request.
2. **Allowed and Prohibited Uses.** You agree that You will not use Your Device to: (a) store or transmit illicit, illegal, or contraband materials; (b) improperly store or transmit other companies' proprietary data; (c) harass another individual or company; or (d) violate any Company policy (including Information Security Policies and Code of Conduct).
4. **Mobile Operating System Alterations.** Maintaining the integrity of mobile operating systems on Devices is crucial for ensuring security and compliance. This policy outlines the requirement to refrain from altering or "jailbreaking" the operating system of personally owned Devices in a manner inconsistent with the manufacturer's end-user agreement.
5. **Allowed Applications.** You agree to comply with Company directives related to prohibited applications and the uninstallation within 24 hours of being notified of certain applications that the Chief Information Security Officer (CISO) deems a risk or threat. You agree not to use ephemeral messaging applications (e.g., WhatsApp, Signal, WeChat, Weixin, etc.) to conduct Company business.
5. **Right to Mandate Security Settings.** You agree to allow the Company, through the mobile device management software (or its equivalent), to push mandatory security settings or applications to Your Device (e.g., requirement to maintain a passcode to access Your Device).
6. **Compliance with Labor Laws.** You agree to use Your access to Company data and communication systems in compliance with local labor laws.
7. **Right to Inspect & Your Consent to Search.** You agree to make Your Device available for inspection or data duplication at any time at the request of an authorized Company representative for any purpose. Legitimate purposes include but are not limited to: (a) electronic discovery for litigation; (b) Company investigations; or (c) cybersecurity incidents. You agree to consent to allow Company, or its authorized representative or agent, to search Your Device.
8. **Comingling of Personal and Business Data.** You acknowledge that placing personal and business data on the same device may result in the Company's access to Your personal data. While Company will use reasonable efforts to avoid duplication and/or viewing of Your personal data, currently available technology does not adequately allow for the separation after it has been comingled. In addition, certain court orders may prohibit the Company from attempting to separate Your personal data from business data in order to comply with a valid legal process.
9. **Termination of Work Relationship & Removal of Data.** Upon termination of Your work relationship with the Company, You agree to cooperate with the Company to immediately remove all Data from Your Device and the ability to access Data from the Device or any other device you may use. If You fail to cooperate, You have been suspected of violating a

Company policy, or Your Device is lost, the Company may remotely delete data from the Device. You will report any lost or stolen Device that was authorized to access Data to infosec@valeurtechnologies.com.au within 24 hours of discovery. You agree You are solely responsible for backing up, on a regular basis, Your personal data.

10. **Survivability.** If any part of this Agreement is found to be unenforceable, all remaining parts will continue to be enforced.
11. **Liability.** You assume full liability for: (a) all costs associated with Your mobile device; (b) any loss or damage that may be caused by Company data or applications; (c) any loss or damage resulting from the Company's configuration of Your mobile device; and, (d) any loss or damage resulting from a Company directive to erase data from Your mobile device.

I have read and agree to the terms and conditions of connecting my personally owned mobile device to Valeur Technologies Inc. and/or its affiliate' systems and data. I understand that failure to comply with this Agreement may result in HR action, up to and including termination of employment.