

<i>Version Control</i>


Version	Issue Date	Author	Reviewed and Approved By	Next Review due on
1.00	27.06.2021	ISMS SPOC	CISO	26.06.2022
2.00	12.04.2022	ISMS SPOC	CISO	11.04.2023
3.00	23.05.2022	ISMS SPOC	CISO	22.05.2023
4.00	28.04.2023	ISMS SPOC	CISO	28.04.2024

<i>Revision History:</i>

Sr. No.	Description of Change	Page No.	Revision by and Date	Approver and Date
1	Initial Release	All	AA and 27.06.2021	Founders and 27.06.2021
2	Annual Review	All	AA and 12.04.2022	Founders and 12.04.2022
3	Semi Annual Review	All	AA and 23.05.2022	Founders and 23.05.2023
4	Annual Review	All	AA and 28.04.2023	Founders and 28.04.2023

The BYOD and Acceptable Use Policy are part of the corporate Information Security Program. Information security policies are the principles that direct managerial decision-making and facilitate secure business operations.

A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent

	<p style="text-align: right;">AceNgage InfoServices</p> <p style="text-align: right;">BYOD Policy with Acceptable Usage ISP-01</p>
---	---

security efforts will be based. They define the appropriate and authorized behaviour for personnel approved to use information assets, such as laptops, tablets and smartphones.

Applicability

The BYOD and Acceptable Use Policy applies to all employees, interns, contractors, vendors and anyone using assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets.

Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

BYOD [Bring Your Own Device] POLICY

This policy provides guidelines for using personally owned devices and related software for corporate use.

BYOD Applicability

The BYOD policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

Furthermore, based on the amount of personally identifiable information (PII) employees work with, management reserves the right to determine which employees can use personally owned devices and which cannot.

General Policy

AceNgage recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by for corporate use:

- Desktop computers
- Laptop computers
- Tablets
- Personal digital assistants (PDAs)
- Smart phones
- Portable music players

Reimbursement



AceNgage will not provide reimbursement for the purchase of personally owned devices. However, some additional costs associated with learning, administering or installing these devices may be considered for reimbursement on case-to-case basis.

This Bring Your Own Device and Acceptable Use Policy is a guideline. It does not address potential compliance issues with Central, state, or local regulatory requirements.

Nor is it meant to be exhaustive or construed as legal advice. Consult your licensed Legal or legal counsel to address possible compliance requirements.

Registering Devices

All personally-owned devices must be registered with the IT department.

End-User Support

As a general rule, users of personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

IT will support personally owned devices as follows:

- The user will be required to allow IT to load security software on each device.
- The user will be required to allow IT to install remote wiping software on each device.
- Upon request, the IT team will install the necessary synchronization software to the user's desktop or notebook computer.

Device Security

The user should follow good security practices including:

- Password protect all personally owned devices
- Do not leave personally owned devices unattended

Release of Liability and Disclaimer to Users

hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability.

In the case of litigation, may take and confiscate a user's personally owned device at any time.



ACCEPTABLE USE POLICY

This policy provides rules for the acceptable use of personally owned devices on the corporate network.

Applicability

The Acceptable Use Policy applies to all employees, contractors, vendors and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

General Policy

Users that wish to access the network using their personally owned computer may do so using only -authorized software and only with the approval of the user's supervisor and the IT department.

Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the network, the user will NOT:

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send junk email or spam to anyone
- Attempt to send a massive amount of email to a specific person or system in order to flood their server

Authorization of Devices

IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

IT will install a digital certificate on each personally owned device, which will authenticate the user.

Third-Party Applications on Devices

IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

As the number of approved applications continually evolves, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading it on the device.

Remote Wiping



While AceNgage does not own the device, they do own all company data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time.

Not only will company data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk.

Furthermore, the user must agree to a full wipe of the personally owned device if they leave. This may result in the loss of both company and personal data on the device.

Reporting Security Concerns

The user agrees to report the following immediately:

- If the device is lost or stolen
- If the device has been attacked with malware, a virus or any other suspicious attack
- Any other security concern with regards to company data

Release of Liability and Disclaimer to Users

AceNgage hereby acknowledges that the use of a personally owned device on the network carries specific risks for which you, as the end user, assume full liability.

Bring Your Own Device (BYOD) and Acceptable Use Policy

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of our organization. It is for this reason we have established our BYOD and Acceptable Use Policy.

All employees are expected to understand and actively participate in this program. encourages its employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

Prior to using personal devices for company purposes, each employee is expected to have read the entire BYOD and Acceptable Use Policy.

If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the BYOD and Acceptable Use Policy.

I have read and understand 's BYOD and Acceptable Use Policy, and I understand the requirements and expectations of me as an employee.

Employee Signature Date



AceNgage InfoServices

BYOD Policy with Acceptable Usage ISP-01

Prepared and Issued by: ISMS SPOC & CISO

Policy reviewed on: 28.04.2023

Next review due on: 28.04.2024