pAI

Policy No.: HR-12 Effective Date: 2025-07-01

Policy Title: IT Acceptable Use & BYOD Policy

Revision No.: 1.0

Supersedes: N/A

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy Statement
5. Procedures / Guidelines
6. Responsibilities
7. Compliance & Consequences
8. Review & Revision History
9. Purpose

This policy defines the acceptable use of pAI’s Information Technology (IT) resources and outlines the guidelines for employees who use their personal devices for company business (Bring Your Own Device - BYOD). Its purpose is to protect pAI’s information assets, ensure a secure and productive work environment, maintain compliance with legal and regulatory requirements, and promote responsible digital citizenship.

1. Scope

This policy applies to all pAI employees (full-time, part-time, permanent, temporary), contractors, consultants, and any other individuals who access or use pAI’s IT resources, networks, systems, software, or data, regardless of location. It also applies to any personal devices used for pAI business.

1. Definitions

| **Term** | **Definition** |
| --- | --- |
| **IT Resources** | All computer hardware, software, networks, data, electronic communication systems (email, instant messaging), internet access, cloud services, and mobile devices owned or managed by pAI. |
| **BYOD (Bring Your Own Device)** | The practice of employees using their personally owned electronic devices (e.g., smartphones, tablets, laptops) to access pAI’s IT resources or data. |
| **Acceptable Use** | The appropriate and permitted ways in which pAI’s IT resources may be utilized for business purposes. |
| **Malware** | Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems (e.g., viruses, ransomware, spyware). |
| **Personal Data** | Any information relating to an identified or identifiable natural person (see Policy HR-13). |
| **Confidential Information** | Any non-public information related to pAI’s business, including but not limited to, trade secrets, proprietary technology, financial data, customer lists, and business strategies (see Policy HR-13). |
| **Unauthorized Access** | Gaining entry to systems, networks, or data without explicit permission. |

1. Policy Statement

4.1 All pAI IT resources are provided primarily for legitimate business purposes. Limited personal use is permitted, provided it does not interfere with job duties, violate any pAI policies, or compromise system security or performance.

4.2 Employees shall use pAI IT resources responsibly, ethically, and in compliance with all applicable laws, regulations, and pAI policies (e.g., Code of Conduct HR-03, Confidentiality & Data Privacy HR-13).

4.3 Employees using personal devices for pAI business (BYOD) must adhere to specific security and data protection requirements outlined in this policy and any associated BYOD agreement.

4.4 pAI reserves the right to monitor all IT resource usage, including electronic communications, to ensure compliance with this policy and for security, operational, and legal purposes.

4.5 Any misuse of IT resources or violation of this policy will result in disciplinary action.

1. Procedures / Guidelines

5.1 Acceptable Use of IT Resources

5.1.1 Business Use Priority: IT resources are primarily for business use. Personal use must be minimal, not interfere with work performance, and not consume excessive network bandwidth or storage.

5.1.2 Prohibited Activities: Employees shall not use pAI IT resources for:

\* Illegal activities (e.g., unauthorized access, harassment, discrimination, copyright infringement).

\* Creating, storing, or transmitting offensive, discriminatory, harassing, or sexually explicit material (see Policy HR-02 and HR-04).

\* Engaging in commercial activities unrelated to pAI business.

\* Gambling or accessing inappropriate websites.

\* Unauthorized downloading or installation of software.

\* Any activity that could damage pAI’s reputation or compromise its security.

5.1.3 Security Practices:

\* Passwords: Employees shall use strong, unique passwords for all pAI systems and not share them. Passwords must be changed regularly as per IT guidelines.

\* Malware Protection: Employees shall not disable security software (e.g., antivirus, firewalls) on company-issued devices. Suspicious emails or links must be reported to IT.

\* Physical Security: Company devices must be secured when not in use and not left unattended in public places.

\* Data Handling: Confidential and personal data must be handled in accordance with Policy HR-13.

5.1.4 Software and Applications: Only pAI-approved and licensed software may be installed on company-issued devices. Unauthorized software installation is prohibited.

5.1.5 Email and Internet Usage:

\* All email communications and internet browsing on pAI networks are company property and subject to monitoring.

\* Employees shall not send or forward chain letters, spam, or unsolicited bulk emails.

\* Professional conduct is expected in all electronic communications.

5.2 Bring Your Own Device (BYOD)

5.2.1 Voluntary Participation: BYOD is a privilege, not a right, and participation is voluntary.

5.2.2 Eligibility: Only devices meeting pAI’s minimum security and compatibility standards, as determined by the IT Department, are eligible for BYOD.

5.2.3 BYOD Agreement: Employees opting for BYOD must sign a formal BYOD Agreement outlining specific terms, including:

\* Security Software: Installation of mandatory pAI security software and mobile device management (MDM) solutions.

\* Data Separation: Understanding that pAI data will be compartmentalized and managed separately from personal data.

\* Remote Wipe: Acknowledgment that pAI has the right to remotely wipe company data from the device in case of loss, theft, or termination of employment.

\* Inspection: Agreement that IT may inspect the device for security compliance.

5.2.4 Data Ownership: All pAI data, intellectual property, and confidential information accessed or stored on a personal device remain the sole property of pAI.

5.2.5 Costs: Employees are generally responsible for the cost of their personal devices, data plans, and maintenance.

Table 1 – Device Usage Guidelines

| **Device Type** | **Acceptable Use** | **Prohibited Use** | **Data Ownership** |
| --- | --- | --- | --- |
| **Company-Issued Devices** | Business purposes, limited personal use | Illegal activities, unauthorized software, excessive personal use | pAI |
| **Personal Devices (BYOD)** | Accessing pAI systems/data as per BYOD agreement | Storing confidential pAI data outside approved apps, circumventing security | Personal device, pAI data on device is pAI's |

1. Responsibilities

| **Role** | **Obligation** |
| --- | --- |
| **Employees** | Adhere to all aspects of this policy. Protect pAI IT resources and data. Report any security incidents or suspicious activity immediately to IT. |
| **IT Department** | Implement and enforce this policy. Provide necessary security tools and support. Monitor IT resource usage for compliance and security. Manage BYOD enrollment and support. |
| **Managers / Supervisors** | Ensure their teams understand and comply with this policy. Address any observed or reported violations. Lead by example in responsible IT use. |
| **Human Resources** | Develop, communicate, and periodically review this policy in conjunction with IT. Advise on disciplinary actions for policy violations. |

1. Compliance & Consequences

7.1 Adherence to this IT Acceptable Use & BYOD Policy is a mandatory condition of employment or engagement with pAI.

7.2 **Violations:** Any violation of this policy, including but not limited to, unauthorized access, misuse of IT resources, security breaches, or non-compliance with BYOD terms, will result in disciplinary action.

7.3 **Disciplinary Action:** Disciplinary measures may include verbal warnings, written warnings, suspension, revocation of IT access, and ultimately, termination of employment, depending on the severity and nature of the violation.

7.4 **Legal Action:** pAI reserves the right to pursue legal action against individuals who engage in illegal activities or cause significant harm to the company through misuse of IT resources.

7.5 **Data Recovery/Wipe:** In cases of policy violation, suspected security breach, or termination of employment, pAI reserves the right to access, copy, or remotely wipe company data from any device (company-issued or personal BYOD) that has accessed pAI IT resources.

1. Review & Revision History

| **Version** | **Date** | **Description** | **Author** |
| --- | --- | --- | --- |
| 1.0 | 2025-07-01 | Initial release | HR Director |