B&S
B&S INVESTMENTS

Human Capital & Culture

Authentication & Password Standards

Purpose

The purpose of this policy is to define the terms under which personally owned devices (smartphones, tablets, laptops) may be used to access B&S Investments› corporate systems, data, and communication tools. This policy enables productivity, mobility, and employee flexibility, while safeguarding the confidentiality, integrity, and availability of corporate data.

As a Saudi-rooted investment group with operations across exhibitions, manufacturing, tourism, creative content, hospitality, and digital ventures, B&S Investments must balance operational convenience with strict cybersecurity controls and regulatory compliance, including PDPL, NCA, and GDPR guidelines.

Scope

This policy applies to all B&S Investments employees, contractors, consultants, and third-party service providers who wish to use their personal devices for work-related tasks. It covers:

- Smartphones and tablets (iOS, Android)
- Personal laptops and computers
- Wearable tech (e.g., smartwatches) when integrated with email or notifications
- Internet of Things (IoT) devices used in operations (if permitted)

This policy applies to access via mobile apps, email clients, web browsers, virtual desktops, and remote connectivity tools.

Policy Statement

B&S Investments permits the use of personally owned devices for approved business purposes, provided that:

- The devices comply with minimum security standards
- Users agree to the terms of this policy through signed consent
- Corporate data accessed via BYOD is protected through encryption, containerization, and mobile device management (MDM)
- IT retains the right to restrict or revoke access at any time for security or compliance reasons

BYOD is a privilege, not a right, and may be suspended if policy conditions are violated.

Roles & Responsibilities

Role	Responsibility
CIO / CISO	Define BYOD strategy, ensure compliance with cybersecurity frameworks, and approve tools
IT Department	Implement MDM, enforce device enrollment, and monitor device compliance
Legal & Compliance	Ensure BYOD aligns with local/international privacy laws, including consent and data access limitations
HR Department	Educate employees on BYOD terms during onboarding and enforce consent collection
Employees / Users	Maintain device security, avoid prohibited actions, and report loss/theft or compromise immediately

Procedures & Implementation

1. **Enrollment & Authorization**
    - All BYOD users must enroll their devices in the company’s MDM platform (e.g., Microsoft Intune, MobileIron)

- Users must sign the BYOD User Agreement, acknowledging data handling and monitoring conditions
- Device access will only be granted upon successful enrollment and configuration

2. 2. Minimum Device Security Standards

All personal devices must meet the following::

Requirement	Description
OS Updates	Devices must run up-to-date operating systems with latest patches installed
Screen Lock	Must have auto-lock enabled with PIN, fingerprint, or facial authentication
Device Encryption	Full-disk encryption must be enabled (e.g., FileVault, BitLocker)
Anti-Malware	Must use reputable antivirus or endpoint protection software (as approved by IT)
No Jailbreaking/ Rooting	Devices that are modified to bypass OS security are strictly prohibited

3. Allowed Applications & Data Access

- Only approved enterprise apps may be installed (e.g., Outlook, Teams, VPN, SharePoint)
- Access is restricted to business-critical platforms through secure gateways
- Corporate email and document access must occur within encrypted containers
- Synchronization of contacts, messages, or documents to personal apps is not allowed

4. Data Security & Monitoring

- All corporate data remains the property of B&S Investments
- IT may remotely wipe company data from any enrolled device upon:
  - Termination of employment
  - Device theft or loss
  - Suspected compromise

- Monitoring includes app usage, system logs, and connection history—but excludes personal content
- IT does not access or monitor personal calls, photos, messages, or non-corporate apps

5. Loss, Theft & Incident Reporting

- Users must report lost, stolen, or compromised devices within 1 hour of discovery
- IT will trigger a remote lock and wipe if corporate data is at risk
- Incidents are documented and reviewed per the Cyber Incident Response Procedure

6. Prohibited Activities

Users may not:

- Share their device or login credentials with others
- Store corporate data on unencrypted third-party apps
- Bypass company-installed security configurations
- Use public cloud storage (e.g., Dropbox, Google Drive) unless explicitly approved
- Access internal systems using unauthorized personal devices

Monitoring & Review

The BYOD Policy is reviewed annually by the CISO, Legal, and HR departments. Interim reviews are triggered by:

- New cybersecurity threats targeting mobile platforms
- Regulatory changes impacting personal device usage
- Expansion of remote work or field operations in new geographies
- Implementation of new device management technologies

BYOD compliance metrics—including enrollment rates, incident frequency, and user violations—are reported quarterly to the Executive Risk Committee.y.

Associated Documents

- Information Security Policy
- IT Access & Acceptable Use Policy
- Cybersecurity Incident Response Procedure
- BYOD User Agreement Form

- Mobile Device Management Configuration Guide
- Data Privacy & Protection Policy
- Third-Party Access Guidelines
- Phishing & Endpoint Security Training Manual
- Remote Work Security Checklist
- Employee Termination Offboarding Checklist