Human Capital & Culture

IT Access & Acceptable Use Policy

Purpose

The purpose of this policy is to ensure that all information technology resources of B&S Investments are accessed and used in a secure, ethical, and business-appropriate manner. This policy defines the standards for acceptable use of IT systems, devices, software, and digital platforms to prevent misuse, data loss, and reputational risk. It enables a balance between operational efficiency and cybersecurity integrity, reflecting the Group's multi-sector footprint and global ambitions.

Scope

This policy applies to all employees, contractors, consultants, interns, and third-party vendors who have authorized access to B&S Investments' IT infrastructure. It covers:

- Desktop and laptop computers
- Mobile phones and tablets
- Email, internet, and messaging systems
- Internal networks and cloud services
- Business applications and collaboration tools
- Removable storage, printers, and teleconferencing systems

Applicable across all sectors including exhibitions, manufacturing, tourism, creative content, hospitality, and digital ventures, both on-premises and remotely..

Policy Statement

B&S Investments provides IT resources to facilitate efficient business operations and collaboration. These resources must be used in a manner that:

- Supports business goals and productivity
- Safeguards company data, systems, and reputation
- Complies with legal, regulatory, and contractual obligations
- Reflects the professional standards expected of all Group personnel

Unacceptable use, including personal misuse, unauthorized installations, or any activity that threatens cybersecurity or workplace professionalism, is strictly prohibited and may result in disciplinary action.

Roles & Responsibilities

Role	Responsibility
Group CIO	Oversees IT governance, access policies, and infrastructure security
IT Department	Manages provisioning, access controls, monitoring, incident handling, and technical enforcement
Department Heads	Approve system access for new joiners, ensure role-based permissions, and escalate access changes or revocations
Employees	Use IT systems responsibly, protect credentials, and report misuse or suspected breaches
HR Department	Coordinates access change workflows during onboarding, role changes, and terminations
Vendors & Consultants	Must comply with acceptable use guidelines in contractual terms and security reviews

Procedures & Implementation

1. **Access Management**
    - **Provisioning**: New users receive access only upon official HR confirmation and departmental approval

- **Principle of Least Privilege:** Users are granted access only to systems and data required for their role
- **Authentication:** Strong passwords and multi-factor authentication (MFA) are mandatory for sensitive systems
- Account Revocation: IT disables user accounts immediately upon contract end, termination, or inactivity beyond 30 days

2. **Acceptable Use Guidelines**
    - IT systems must be used solely for authorized business purposes
    - Company email must not be used for personal, political, or unauthorized external communications
    - Downloading or installing unapproved software, applications, or extensions is strictly prohibited
    - Company systems must not be used to access, store, or distribute inappropriate, offensive, or illegal content
    - Users must lock workstations when unattended and avoid leaving confidential information visible
    - Use of cloud storage or communication tools (e.g., Google Drive, WhatsApp) must be aligned with company-approved platforms
    - Removable media (e.g., USB drives) may only be used if encrypted and scanned for malware

3. **Remote & Mobile Access**
    - Only company-issued or authorized devices may be used for remote work
    - VPN connections are required for external access to internal systems
    - Public Wi-Fi must be avoided or used with caution, and only with encrypted VPN sessions
    - Mobile devices must be configured with security features including auto-lock, biometric access, and remote wipe capability

4. **Monitoring & Logging**
    - All system usage is monitored for security, compliance, and performance purposes
    - Internet access, downloads, and email traffic are logged through secure gateways
    - Users have no expectation of privacy when using company devices or systems

- Any violation may be investigated, and logs submitted to HR or Legal for disciplinary review

5. **Prohibited Activities**
    - Examples of prohibited actions include (but are not limited to):
    - Sharing passwords or login credentials
    - Attempting to bypass access controls or monitoring tools
    - Engaging in phishing, malware distribution, or social engineering
    - Participating in personal online trading, gambling, or illegal file sharing
    - Unauthorized use of AI tools or external code execution platforms without review

Monitoring & Review

The IT Access & Acceptable Use Policy is reviewed annually by the CIO, CISO, and Legal Department. Interim reviews may be triggered by:

- Regulatory or contractual changes (e.g., NCA, PDPL, or GDPR updates)
- Discovery of misuse or internal policy breach
- New system rollouts, remote work policy changes, or changes to risk posture

Metrics such as security incident frequency, usage violations, and phishing simulation results will inform ongoing revisions and enforcement.

Associated Documents

- Information Security Policy
- Remote Work & Bring Your Own Device (BYOD) Guidelines
- Password Management Policy
- Third-Party Access Control Checklist
- Data Classification & Handling Guidelines
- User Access Request Form
- Termination Exit Checklist (IT Access Revocation)
- Email & Communication Policy
- Cybersecurity Incident Response Plan