Human Capital & Culture

Information Security Policy

Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of all information assets and systems owned or managed by B&S Investments. As a Saudi-rooted, globally active multi-sector holding group, safeguarding digital infrastructure, proprietary information, and client data is vital to business continuity, regulatory compliance, and stakeholder trust..

Scope

This policy applies to all employees, contractors, consultants, vendors, and third parties with access to B&S Investments' information systems, data, and digital infrastructure. It covers all business units, including exhibitions, manufacturing, tourism, creative content, hospitality, and digital ventures.

- The policy governs:
- Data access, usage, and storage
- Network and infrastructure protection
- User authentication and identity management
- Device and endpoint security
- Email, internet, and system usage
- Cyber incident response and recovery

B&S

Policy Statement

B&S Investments is committed to implementing industry-aligned security standards to defend against internal and external threats, ensure data integrity, and maintain secure business operations. Every user of the company's information systems is accountable for protecting sensitive data and reporting security concerns in a timely manner.

- Core principles include:
- Only authorized users have access to relevant systems and data
- Sensitive data must be classified, encrypted, and monitored
- Cybersecurity measures must be updated regularly to defend against evolving threats
- Employees must be trained and empowered to prevent security breaches
- All systems and access are logged, monitored, and auditable

Failure to comply with this policy may result in disciplinary action or legal consequences.

Roles & Responsibilities

Role	Responsibility
Board of Directors & Executive Leadership	Oversee enterprise-wide cybersecurity strategy and risk mitigation investments
Chief Information Security Officer (CISO)	Owns information security strategy, standards, threat detection, and incident response
IT Department	Manages technical controls, infrastructure security, system patching, and access provisioning
Department Heads	Ensure team members follow access protocols and report any system misuse or anomalies
All Employees	Follow secure practices, report suspicious activities, and protect passwords and data
Vendors & Third Parties	Adhere to security terms within contractual agreements and undergo risk assessments

Procedures & Implementation

1. **Access Management**
    - All users are assigned role-based access rights using the principle of least privilege
    - Access to sensitive systems or data requires managerial approval and multi-factor authentication (MFA)
    - Account credentials must not be shared under any circumstance
    - Terminated users are deactivated within 24 hours of exit by IT
2. **Data Classification & Protection**
    - All data must be classified into one of the following categories: Public, Internal, Confidential, Restricted
    - Confidential and Restricted data must be encrypted in transit and at rest
    - Sensitive data must not be stored on personal devices or cloud services not approved by IT
3. **Device & Endpoint Security**
    - All corporate devices must have approved antivirus, encryption, and endpoint protection tools installed
    - USB devices must be scanned or disabled by default
    - Lost or stolen devices must be reported to IT immediately for remote wipe protocols
4. **Network & Infrastructure Controls**
    - Firewalls, intrusion detection systems (IDS), and VPNs are used to secure internal networks
    - Public Wi-Fi use for company business is discouraged without VPN connection
    - All systems undergo periodic penetration testing and vulnerability assessments
5. **Acceptable Use of Systems**
    - Email and internet use must be professional and business-related
    - Employees must not access prohibited websites, download unauthorized software, or install unverified applications
    - Phishing and scam emails must be reported immediately using the “Report Phishing” tool

6. **Incident Response & Breach Reporting**
    - Any suspected data breach or cyber threat must be reported to the CISO or IT helpdesk within 1 hour
    - The Incident Response Team (IRT) will isolate affected systems, assess damage, and coordinate recovery
    - A post-incident review will be conducted within 72 hours of resolution
7. **Training & Awareness**
    - All employees must complete annual information security training
    - Additional phishing simulations, tabletop exercises, and department-specific modules will be delivered throughout the year
    - Policy updates and threat advisories will be distributed through the internal security bulletin

Monitoring & Review

The Information Security Policy is reviewed bi-annually by the CISO and audited internally in coordination with the Internal Audit function. Key triggers for interim review include:

- Regulatory or legal changes (e.g., PDPL, GDPR)
- Emerging cyber threats or attack vectors
- Implementation of new systems, tools, or digital platforms
- Post-incident lessons or audit findings

Security metrics (e.g., incident response time, phishing click rates, patch compliance) are tracked and reported quarterly to the Board's Audit & Risk Committee.

Associated Documents

- Cybersecurity Risk Register
- Data Classification & Handling Guidelines
- Secure Password Management SOP
- Acceptable Use Policy
- Incident Response Plan (IRP)
- Business Continuity & Disaster Recovery Policy
- Third-Party Risk Management Guidelines

- Information Security Awareness Training Manual
- Encryption & Endpoint Security Protocol
- Vendor Security Evaluation Checklist