Human Capital & Culture

Cyber Incident Response Procedure

Purpose

The purpose of this procedure is to provide a clear, structured, and swift approach for detecting, reporting, responding to, containing, and recovering from cybersecurity incidents across B&S Investments. It ensures business continuity, minimizes damage, protects data assets, and supports compliance with regulatory obligations including Saudi Arabia's PDPL, NCA guidelines, and international data breach laws (e.g., GDPR).

Scope

This procedure applies to all B&S Investments entities, business units, and subsidiaries, including exhibitions, manufacturing, tourism, creative content, hospitality, and digital ventures. It applies to:

- All employees, contractors, and third-party users
- All digital assets including networks, endpoints, cloud services, databases, IoT devices, and operational technology
- All cybersecurity incidents regardless of origin (internal or external)

Incidents covered include:

- Malware or ransomware attacks
- Unauthorized access or account compromise

- Data breach or leakage (including PII, financial, or client data)
- Denial-of-Service (DoS/DDoS) attacks
- Insider threats or sabotage
- Phishing or social engineering attempts
- System misconfigurations or vulnerability exploitation..

Policy Statement

B&S Investments maintains a proactive and disciplined approach to cyber incident response. All employees and stakeholders must act immediately and in coordination with the Information Security team to isolate threats, preserve evidence, and restore normal operations. No incident should be ignored or handled informally.

- Key principles include:
- Immediate containment and escalation
- Preservation of forensic evidence
- Rapid stakeholder communication
- Root cause analysis and corrective action
- Regulatory and legal compliance
- Post-incident review and policy improvement

Roles & Responsibilities

Role	Responsibility
CISO (Incident Commander)	Leads incident response operations, approves containment actions, and escalates to senior leadership
Cybersecurity Incident Response Team (CIRT)	Executes technical response activities (detection, isolation, analysis, recovery, forensic investigation)
IT Department	Provides infrastructure access, technical support, and implements emergency controls
Legal & Compliance	Assesses legal implications, manages regulatory reporting, and supports law enforcement liaison

Role	Responsibility
Communication/PR	Prepares internal and external communication aligned with executive guidance
Business Unit Heads	Support containment efforts and execute business continuity plans where applicable
All Employees	Report suspicious activities or breaches immediately to IT/ Security helpdesk

Procedures & Implementation

1. **Detection & Identification**
    - Incidents may be detected via automated systems (e.g., intrusion detection, antivirus alerts), employee reports, third-party notifications, or audit findings
    - Indicators of compromise include unusual logins, system slowdown, unauthorized file access, or unknown devices on the network
    - Initial responder completes the **Cyber Incident Report** Form and alerts the CIRT immediately
2. **Classification & Prioritization**
    - Incidents are categorized by severity (Low, Medium, High, Critical) based on:
        - Impact on operations
        - Sensitivity of affected data
        - Extent of compromise or propagation
        - Legal/regulatory exposure
    - The Incident Commander assigns a response lead and initiates the appropriate playbook
3. **Containment (Short-Term & Long-Term)**
    - Short-Term Containment:
        - Disconnect affected devices
        - Disable compromised accounts
        - Block malicious IPs/domains

- Stop data exfiltration or system spread
- Long-Term Containment:
  - Apply patches
  - Strengthen firewall or rule sets
  - Deploy endpoint detection and response (EDR) solutions
  - Revoke unnecessary privileges

4. **Eradication & Recovery**
   - Remove malware, unauthorized software, or backdoors
   - Validate system integrity
   - Restore from clean backups
   - Conduct full system scans
   - Reactivate accounts and services with MFA enforcement
   - Monitor for recurrence and unusual post-incident activity

5. **Communication & Escalation**
   - Notify executive leadership for incidents rated High or Critical
   - For data breaches involving PII or regulated data:
     - Notify the Saudi Data & AI Authority (SDAIA) within 72 hours
     - Notify affected data subjects if risk of harm is assessed
   - External communications must follow approved messaging only via the PR and Legal teams

6. **Documentation & Evidence Handling**
   - All actions must be logged in the **Cyber Incident Logbook**
   - Screenshots, logs, system images, and communications are preserved for forensic investigation
   - Chain of custody is maintained for any evidence shared with external investigators or regulators

7. **7. Post-Incident Review & Reporting**
   - A formal **Post-Incident Review (PIR)** is conducted within 10 business days
   - Lessons learned are documented in the **Incident Closure Report**, including:
     - Root cause analysis
     - Timeline of events
     - Gaps identified

    - Recommendations
- Policies, SOPs, and systems are updated as needed
- Training is conducted if user error contributed to the incident

Monitoring & Review

The Cybersecurity Incident Response Procedure is reviewed bi-annually by the CISO and Internal Audit. The following triggers may prompt an interim review:

- Regulatory updates (e.g., changes in PDPL or GDPR)
- Major incident or breach
- Introduction of new IT infrastructure or cloud services
- M&A activity or expansion into high-risk markets

Incident trends and metrics (e.g., mean time to detect/respond/recover, incident frequency by type) are reported quarterly to the Audit & Risk Committee.

Associated Documents

- Information Security Policy
- Cyber Incident Report Form
- Cybersecurity Incident Logbook
- Incident Playbooks (Ransomware, Phishing, DoS, Insider Threats)
- Forensic Investigation Protocol
- Business Continuity & Disaster Recovery Policy
- Data Breach Notification SOP
- PR & Crisis Communication Template
- Post-Incident Review Template
- Security Awareness Training Manual