Risk & Compliance

Crisis Management & Business Continuity Policy

Purpose

The purpose of this policy is to establish a standardized and proactive approach to crisis management and business continuity across B&S Investments. As a Saudi-rooted, multi-sector holding group operating in exhibitions, manufacturing, tourism, creative content, hospitality, and digital ventures, B&S Investments must ensure operational stability and rapid recovery from any disruption. This policy safeguards business integrity, protects stakeholder confidence, and upholds compliance with legal, financial, and contractual obligations under adverse conditions.

Scope

This policy applies to all business units, subsidiaries, departments, and personnel of B&S Investments in both domestic and international markets. It covers natural disasters, cyberattacks, public health emergencies, supply chain disruptions, critical system failures, security breaches, reputational crises, and any other unforeseen event that may impair business operations.

- The policy includes governance over:
- Crisis preparedness and response
- Business continuity planning (BCP)
- Emergency communication
- Disaster recovery (DR)
- Incident escalation and post-incident review.

Policy Statement

B&S Investments is committed to building organizational resilience and ensuring the uninterrupted delivery of critical functions during and after disruptive events. Crisis management and business continuity are core components of our risk management strategy and must be embedded into operations, decision-making, and culture.

The company will:

- Identify and classify potential threats to operations
- Develop and maintain functional business continuity and recovery plans
- Establish crisis response teams and escalation protocols
- Train personnel and test continuity plans regularly
- Ensure transparent, timely communication with internal and external stakeholders during a crisis
- Maintain compliance with all regulatory requirements related to business continuity

Every department must be capable of identifying vulnerabilities, triggering appropriate response plans, and executing predefined recovery measures in alignment with this policy..

Roles & Responsibilities

Role	Responsibility
Board of Directors	Reviews organizational crisis readiness and provides oversight on major incidents and recovery performance
Group CEO	Leads the Crisis Leadership Team and is accountable for strategic crisis response and public-facing decisions
Chief Risk Officer (CRO)	Owns the enterprise-wide business continuity framework; ensures plans are developed, tested, and updated
Crisis Management Team (CMT)	Cross-functional team activated during crises; responsible for coordination, incident response, communication, and recovery management
IT & Cybersecurity	Maintains the Disaster Recovery Plan for critical systems, including data recovery and infrastructure continuity
Business Unit Heads	Ensure local BCPs are documented, team roles are assigned, and periodic testing is conducted

Role	Responsibility
People & Culture Department	Supports employee safety, emergency procedures, and internal communication during a crisis
Facilities & EHS	Manages on-site physical response (e.g., evacuation, fire safety, access control) and ensures compliance with health and safety regulations
All Employees	Must be familiar with local response plans, attend required training, and follow procedures during incidents

Procedures & Implementation

1. **Risk Assessment & Business Impact Analysis (BIA)**
    - Every business unit must conduct a Business Impact Analysis to:
        - Identify critical functions and interdependencies
        - Assess downtime tolerances and recovery time objectives (RTOs)
        - Define Recovery Point Objectives (RPOs) for IT and data systems
    - Risk scenarios must be aligned with enterprise risk assessments and updated annually
2. **Business Continuity Plans (BCPs)**
    - Each department must maintain an operational BCP, which includes:
        - Critical processes and backup procedures
        - Contact lists and emergency resources
        - Alternate sites or remote work protocols
        - Recovery priorities and escalation paths
    - All BCPs are reviewed by the Risk team and validated for completeness
3. **Crisis Management Framework**
    - A Crisis Management Team (CMT) is activated during major disruptions, led by the Group CEO or delegate
    - Crisis categories are defined as:
        - Level 1: Localized disruption (managed by BU leadership)
        - Level 2: Sector-wide or regional impact (requires CMT coordination)

- Level 3: Enterprise-wide, regulatory, or reputational threat (Board involvement)

- Crisis simulation exercises are conducted bi-annually, including tabletop and live drills

4. **Emergency Communication Protocol**

   - All internal and external communications during a crisis must follow the Emergency Communication Plan, which includes:
     - Designated spokespersons
     - Pre-approved messaging templates
     - Stakeholder notification lists (clients, regulators, media, employees)
   - A central Crisis Information Hub (internal portal) will be used to share updates in real-time

5. **Disaster Recovery (IT & Systems)**

   - The IT Disaster Recovery Plan (DRP) ensures:
     - Restoration of systems within RTO/RPO timelines
     - Secure backup infrastructure with geographic redundancy
     - Incident detection, response, and forensic capabilities for cyber events
   - Cloud-based platforms and data integrity controls are reviewed quarterly

6. **Post-Incident Review & Continuous Improvement**

   - Following any significant incident or drill:
     - A formal After-Action Review (AAR) must be conducted
     - Lessons learned are captured in a Post-Incident Report
     - Improvement actions are assigned with timelines and owners
   - Findings are reported to the Board and embedded into the next BCP revision cycle

Monitoring & Review

The Crisis Management & Business Continuity Policy is reviewed annually by the Chief Risk Officer in collaboration with the Group COO, IT Security, and the Compliance Office. Performance metrics include:

- Plan completeness and testing frequency

- Crisis response time vs. RTOs
- Staff training completion rates
- Frequency and severity of business disruptions

Audit findings, industry developments, or regulatory updates may trigger additional reviews. Any updates to the policy or continuity plans will be cascaded across business units and included in training materials..

Associated Documents

- Enterprise Risk Management (ERM) Policy
- IT Disaster Recovery Plan
- Emergency Communication Plan
- Business Impact Analysis (BIA) Template
- Facility Emergency Response Plan
- Crisis Management Team Charter
- Internal Audit Reports on BCP Effectiveness
- Remote Work & Contingency Access Protocol
- Whistleblower Protection Policy
- Regulatory Compliance Matrix (Continuity Obligations)