

Business Continuity & Health & Safety Policy

A Summary



Introduction

KFH Capital is committed to ensuring the safety, resilience, and operational continuity of our organization, employees, and stakeholders. Our Business Continuity and Health & Safety Policies are designed to prepare for, respond to, and recover from any disruption—whether natural disasters, cyber incidents, or operational challenges—while fostering a culture of safety, compliance, and continuous improvement.

In essence, a BCMS ensures KFH Capital is prepared for unforeseen events, reducing the impact of disruptions while enabling rapid recovery. It provides a systematic approach to managing business continuity, fostering trust and confidence among all stakeholders.

Our Commitment

- To safeguard people, assets, and critical operations.
- To comply with all relevant legal and regulatory requirements.
- To build trust among customers, partners, and the wider community.
- To promote a proactive approach to risk management and organizational resilience.

Purpose of the Policy

This policy establishes a framework for:

- Protecting the health and safety of all employees and visitors.
- Ensuring the continuity of essential business operations during and after disruptive events.
- Meeting regulatory and legal obligations in the State of Kuwait and beyond.
- Supporting the strategic objectives and long-term sustainability of KFH Capital.

Scope & Applicability

Scope of the Policy

This policy applies to:

- All employees, business units, and third-party partners, involved in delivering essential services.
- All KFH Capital offices, staff, and operations, including directors, executives, and temporary workers.
- All forms of information and assets, whether physical, digital, or intellectual.

Types of Disruptions Covered

The policy addresses a wide range of potential disruptions, including:

- Natural disasters (e.g., fire, flood, earthquake, severe weather)
- Cybersecurity incidents (e.g., data breaches, ransomware, IT system failures)
- Operational failures (e.g., power outages, supply chain disruptions)
- Public health emergencies (e.g., pandemics, biohazards)
- Security threats (e.g., unauthorized access, workplace violence)
- Regulatory and compliance failures

Exclusions

- Non-critical business units and third parties are required to have their own continuity plans, but their ability to support KFH Capital is addressed in service agreements.
- Confidential and sensitive operational details are excluded from this public summary.

Objectives & Guiding Principles

Key Objectives

Our Business Continuity and Health & Safety Policy is guided by the following objectives:

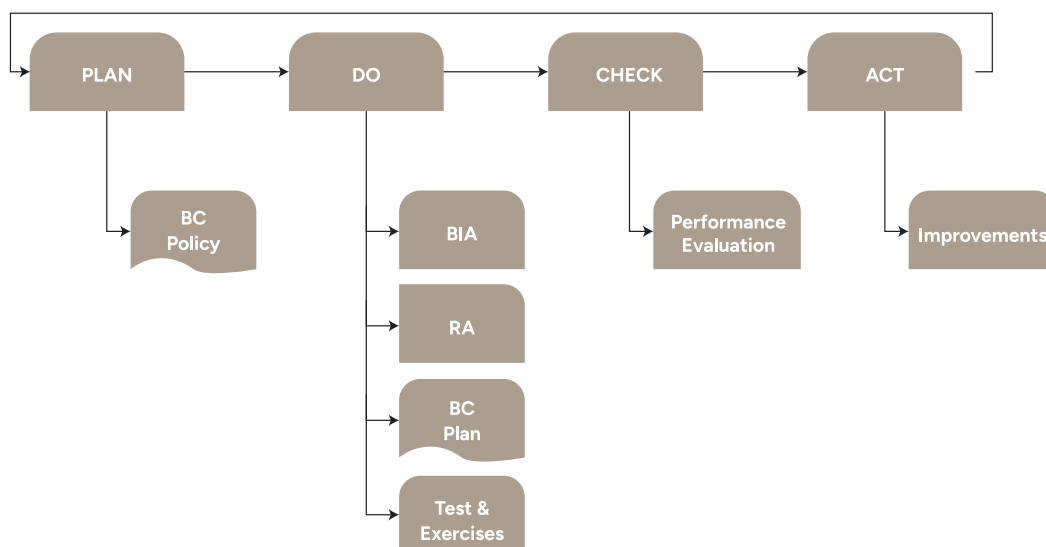
- **Continuity of Critical Services:** Maintain delivery of essential products and services during disruptions.
- **Risk Management:** Identify, assess, and mitigate risks to minimize impact.
- **Resilience:** Enhance the organization’s ability to adapt and recover quickly.
- **Stakeholder Protection:** Safeguard the interests of employees, customers, suppliers, and regulators.
- **Compliance:** Align with legal, regulatory, and contractual requirements.
- **Continuous Improvement:** Regularly test, review, and refine our plans and strategies.

Guiding Principles

- **Proactive Risk Identification:** Early detection and assessment of potential threats.
- **Regular Training and Awareness:** Ongoing education and drills for all staff.
- **Clear Roles and Responsibilities:** Defined accountability at every level.
- **Effective Communication:** Timely and accurate information sharing during crises.
- **Ongoing Review:** Annual and post-incident reviews to ensure relevance and effectiveness.

PLAN-DO-CHECK-ACT FRAMEWORK

The Business Continuity framework applies the PLAN (establish), DO (implement and operate), CHECK (monitor and review) and ACT (maintain and improve) cycle to implement, maintain and continually improve the effectiveness of KFH Capital BCMS.



Governance & Roles

Business Continuity Governance Structure

KFH Capital has established a robust governance structure to ensure effective management of business continuity and health & safety:

- **Crisis Management Team (CMT):** Provides strategic direction, oversees crisis response, and ensures alignment with organizational objectives.
- **Emergency Response and Recovery Teams:** Coordinate preparedness, response, and recovery activities across all business units.
- **Business Continuity/Risk Champions:** Act as focal points within each business unit for continuity planning and execution.
- **Health & Safety Team:** Ensures workplace safety, compliance, and emergency preparedness.

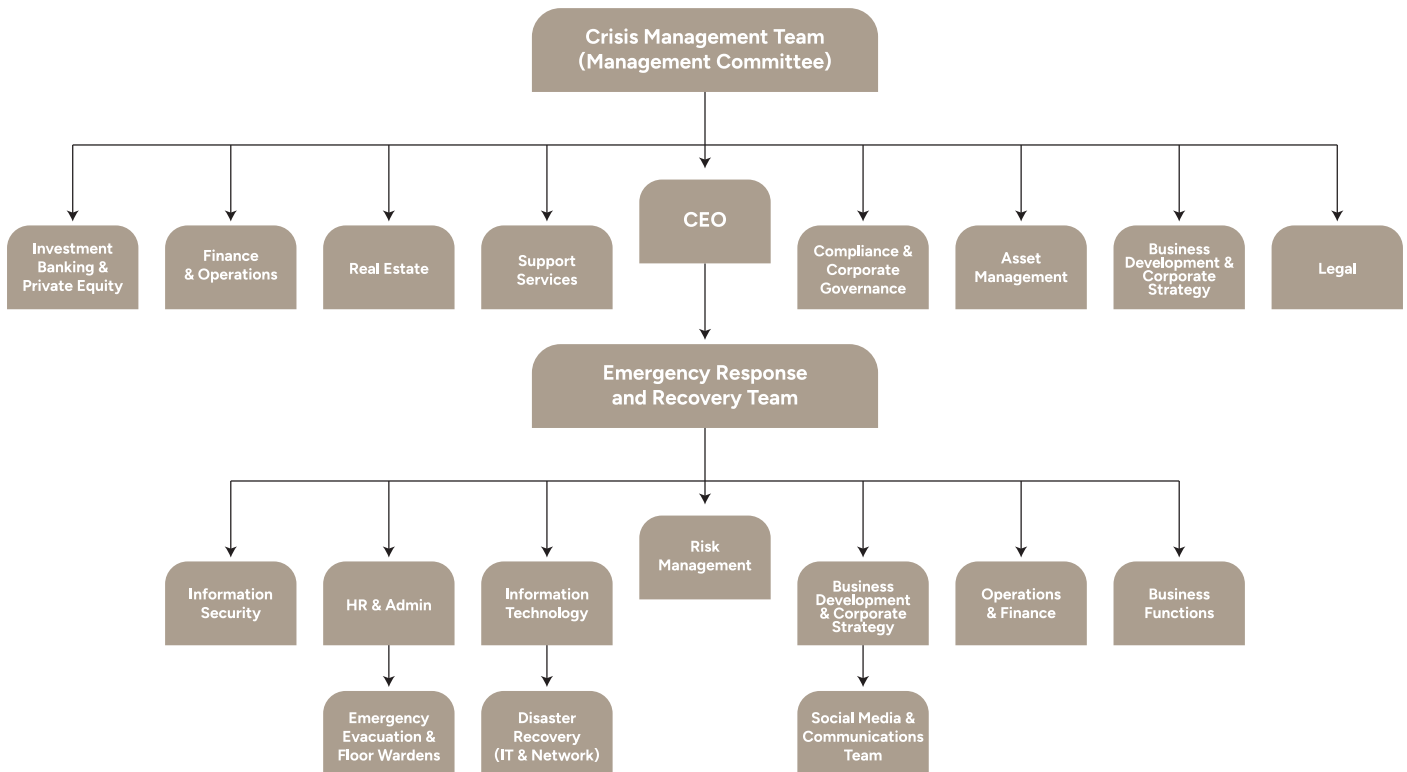
Roles & Responsibilities

- **All Employees:** Responsible for compliance, reporting incidents, and participating in training and drills.
- **Management:** Ensures policy implementation, resource allocation, and regular reviews.
- **Specialized Teams:** Conduct drills, maintain plans, and support recovery efforts.
- **Third-Party Partners:** Required to support KFH Capital's continuity objectives as per contractual agreements.

To achieve the KFHC Business Continuity objectives, the organization has implemented a two-tiered Business Continuity Management (BCM) hierarchy, each with distinct roles and responsibilities:

- **Crisis Management Team (Strategic Level):** Responsible for high-level decision-making, strategic guidance, and liaising with external stakeholders.
- **Emergency Response and Recovery Teams (Tactical Level):** Focused on coordinating response efforts, resource allocation, and implementing response plans. Tasked with executing response activities, ensuring business functions resume in accordance with recovery objectives.

KFH Capital Business Continuity Governance Structure



Preparedness & Response

Preparedness Measures

- **Risk Assessments & Business Impact Analyses:** Regularly conducted to identify critical processes, assets, and potential threats.
- **Training & Drills:** Mandatory participation in scenario-based exercises, including evacuation, lockdown, and first aid drills.
- **Plan Maintenance:** Annual reviews and updates to reflect changes in risks, regulations, and business operations.

Response Strategies

- **Incident Response:** Clear procedures for responding to emergencies, including evacuation, communication, and recovery.
- **Recovery Plans:** Strategies to restore operations, protect data, and minimize downtime.
- **Communication:** Timely and accurate updates to employees, stakeholders, and the public during crises.
- **Coordination with Authorities:** Collaboration with local emergency services and regulatory bodies as needed.

KFH Capital Business Continuity Capabilities

KFHC currently possesses the following key capabilities to support its Business Continuity Plan (BCP) and enhance organizational resilience:

- **Third-Party Co-location of IT Infrastructure**

The organization's critical IT systems are strategically located at a highly secure and resilient facility that serves as the central hub for Kuwait's networking infrastructure. This ensures enhanced security, strict access controls, and protection against physical threats. All IT aspects of disaster recovery will be ensured as per applicable IT and IT Disaster recovery documents.

- **IT Disaster Recovery Site**

KFHC has established a robust IT infrastructure by maintaining a Primary Data Centre (PDC) and a Disaster Recovery (DR) Site to ensure the availability, resilience, and continuity of critical business operations. The Primary Data Centre serves as the core hub for hosting essential IT systems, applications, and data, supporting day-to-day operations with high availability and security measures. In the event of an unforeseen disruption, the Disaster Recovery Site will be activated as a failover facility, enabling the rapid restoration of services and minimizing downtime. Both sites are equipped with advanced security controls, redundant power and cooling systems, and regular data replication mechanisms to ensure seamless business continuity. This dual-site approach enhances the organization's ability to respond to potential disruptions, ensuring operational resilience and compliance with regulatory and business continuity requirements.

- **Security Incident Response Plan**

A structured incident response plan is in place to address various emergency scenarios, including cyber-attacks, DDOS attacks, data breach, and operational disruptions. The plan includes defined roles, responsibilities, and escalation procedures to facilitate a coordinated response.

Scenario based Response Priorities

Scenarios	Key Focus Areas	Key Action Priorities
Civil Disorder	Staff Safety, Communication, Security	-Evacuate or shelter in place Use emergency communications Lock down Office valuables and data Notify government authorities Conduct headcount post-incident
IT Systems Unavailable	Continuity, Recovery, Communication	- Identify cause and notify management - Activate DR plan and backups - Communicate recovery timelines - Restore and validate systems

<p>Power Outage</p>	<p>Backup Power, Safety, Communication</p>	<ul style="list-style-type: none"> - Activate UPS/generators as available - Prioritize essential systems - Inform staff and coordinate with Building Admin - Ensure emergency lighting - Arrange remote work if needed
<p>Geopolitical Disruption</p>	<p>Staff Safety, Remote Work, Continuity</p>	<ul style="list-style-type: none"> - Evacuate or relocate staff - Enable remote work & - Secure assets and data - Maintain crisis communication - Focus on critical operations
<p>Vendor Support Disruption</p>	<p>Supplier Risk, Continuity</p>	<ul style="list-style-type: none"> - Identify critical vendors - Diversify suppliers - Communicate with vendors - Explore local sourcing - Affected function to conduct Business Impact Analysis and report
<p>Severe Weather</p>	<p>Staff Safety, Facility Prep, Remote Work</p>	<ul style="list-style-type: none"> - Notify staff and enable remote work - Secure facilities - Ensure backup power - Coordinate with vendors and authorities
<p>Fire or Earthquake</p>	<p>Evacuation, Safety, Continuity</p>	<ul style="list-style-type: none"> - Evacuate and guide to assembly point (Parking of Baitak Tower in the ground floor) - Use emergency communications - Provide first aid - Backup data and shut down IT -Relocate to work from home

Health & Safety Focus

Workplace Safety

- **Commitment:** A safe and healthy work environment is fundamental to employee well-being and operational success.
- **Compliance:** Adherence to Kuwait Labor Law and international standards.
- **Hazard Identification:** Employees are encouraged to report hazards and unsafe conditions.
- **Safety Inspections:** Regular assessments to identify and mitigate risks.

Emergency Preparedness

- **Evacuation Procedures:** Clearly marked exits, designated assembly points, and regular evacuation drills.
- **First Aid Resources:** Accessible first aid kits and trained personnel on every floor.
- **Emergency Contacts:** Displayed prominently throughout the workplace.
- **Training:** All employees receive health & safety orientation and participate in regular drills.

Continuous Improvement & Compliance

Continuous Improvement

- **Testing:** Regular testing of business continuity and disaster recovery plans.
- **Post-Incident Reviews:** Analysis of incidents to identify lessons learned and update procedures.
- **Ongoing Training:** Continuous education and awareness programs for all staff.

Compliance & Review

- **Alignment with Standards:** Compliance with ISO 22301 (Business Continuity Management), ISO 31000 (Risk Management), and other relevant standards.
- **Annual Reviews:** Policy and plan updates to ensure ongoing relevance and effectiveness.
- **Documentation:** Transparent reporting and record-keeping of all continuity and safety activities.

Commitment to Transparency

We are committed to keeping our stakeholders informed and engaged. All relevant Business Continuity Updates will be communicated in accordance with our policies and procedures through our website and official channels.