Business Continuity Policy

The purpose of this Business Continuity Policy is to ensure that NIST Global is prepared to respond to, manage, and recover from disruptions that may affect its people, operations, services, information assets, reputation, or financial stability. The policy provides a structured framework to maintain continuity of critical business activities and minimize adverse impacts on clients, stakeholders, and the organization.

This policy applies to:

- All departments, functions, and locations of NIST Global
- All business models, including Business to Customer (B2C), Business to Business (B2B), and Business to Government (B2G)
- All employees, Directors, Department Heads, contractual staff, and authorized third parties

The policy addresses disruptions arising from people, operational, technological, financial, environmental, and reputational risks.

Policy Structure

This document describes the key elements of Business Continuity at **NIST Global** and sets out the organization's commitment and high-level standards for ensuring continuity of critical activities during disruptions.

It is divided into the following sections:

- **Business Continuity Planning Policy** – NIST Global's business continuity commitment, objectives, governance approach, and organizational context.
- **Business Continuity Planning Standards** – the high-level continuity standards and arrangements through which NIST Global prepares for disruptions, maintains resilience, and supports recovery.
- **Business Continuity Monitoring and Improvement** – the processes for risk assessment, business impact consideration, recovery planning, awareness, training, periodic review, and continuous improvement of business continuity arrangements.

Business Continuity Planning Policy

a. Policy Objectives

The objectives of this policy are to:

- Ensure continuity of critical services during disruptions
- Protect employee safety and stakeholder interests
- Safeguard organizational data, client information, and intellectual property
- Reduce dependency on single individuals, systems, or vendors
- Maintain client confidence, brand reputation, and regulatory commitments
- Enable timely recovery and return to normal operations

b. Organizational Context

NIST Global is a service-driven Health, Safety, and Environment (HSE) organization providing international safety training, corporate training, auditing, consulting, staffing, and digital EHS solutions. Business continuity is dependent on:

- Availability of qualified leadership and skilled personnel
- Valid accreditations and authorizations from international bodies
- Reliable service delivery across B2C, B2B, and B2G segments
- Secure and resilient technology platforms and data systems
- Financial stability and sustained business development

c. Governance and Responsibilities

Overall accountability for Business Continuity rests with the Board of Directors.

Responsibilities include:

- Directors providing strategic direction and critical decision-making during disruptions
- Senior management implementing and monitoring continuity measures
- Department Heads ensuring continuity within their functions
- Employees complying with continuity controls and reporting incidents promptly

Clear delegation of authority shall be established to ensure continuity during leadership absence.

Business Continuity Planning Standards

a. Leadership and Workforce Continuity

To address dependency on key individuals, NIST Global shall:

- Define alternate responsibilities for Directors during prolonged absence
- Establish interim leadership arrangements in the event of multiple leadership unavailability
- Implement department-level backup planning for critical roles
- Promote cross-training and structured knowledge transfer
- Manage risks arising from multiple or bulk employee resignations, particularly in client-facing functions

b. Business Operations Continuity

❖ **B2C Operations**

Continuity measures shall address:

- Decline in enrolments or sales for international safety training
- Risks associated with non-renewal, suspension, or withdrawal of accreditations

- Use of alternate delivery models and market diversification strategies

❖ **B2B Operations**

Continuity measures shall address:

- Delivery challenges under tight client timelines
- Reduced order inflow or high dependency on limited clients
- Effective resource planning and prioritization of critical commitments

❖ **B2G Operations**

Continuity measures shall address:

- Delays, suspension, or cancellation of government projects
- Approval dependencies and payment delays
- Controlled dependency on government contracts through diversification

c. Technology, Data, and Information Security Continuity

NIST Global recognizes information and technology as critical assets and shall ensure continuity through:

- Protection against cyber threats, hacking, and unauthorized access
- Controls to ensure data confidentiality, integrity, and availability
- Measures to address theft or loss of devices and unauthorized data deletion
- Defined incident response and system recovery responsibilities
- Contingency planning for third-party cloud or service provider outages

Information security and IT continuity controls shall be aligned with the principles of ISO/IEC 27001 Information Security Management System (ISMS), including access control, incident management, backup, and recovery mechanisms.

d. Crisis and Disruption Management

The organization shall maintain preparedness for major disruption scenarios, including:

- Pandemics or widespread health emergencies
- Natural disasters such as fire, earthquake, or other physical incidents
- Incidents occurring during employee travel for audits, inspections, or client engagements

Employee safety shall remain the highest priority during all crisis situations.

e. Financial and Commercial Resilience

To ensure financial continuity, NIST Global shall:

- Monitor cash flow and sustain operations during prolonged low-business periods
- Manage pricing pressures arising from aggressive competition
- Implement cost controls and prioritize essential expenditures
- Maintain financial buffers to support continuity during downturns

f. Communication and Reputation Management

Effective communication during disruptions shall be ensured through:

- Clear internal communication with employees and leadership
- Timely and consistent external communication with clients, partners, and authorities
- Proactive response to misinformation, false allegations, or reputational threats
- Protection of brand credibility through controlled and transparent messaging

Business Continuity Monitoring and Improvement

a. Risk Assessment and Business Impact Consideration

NIST Global shall periodically:

- Identify risks that may disrupt business operations
- Assess potential impacts on people, services, revenue, and reputation
- Prioritize critical functions and services for continuity planning

b. Recovery Strategy and Timeframes

The organization shall define:

- Acceptable timeframes for restoring critical operations
- High-level recovery strategies for key disruption scenarios
- Phased return to normal operations based on business priorities

c. Awareness, Training, and Preparedness

NIST Global shall:

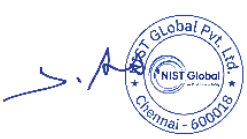
- Promote awareness of business continuity responsibilities
- Ensure leadership and key personnel understand continuity expectations
- Maintain readiness to activate alternate working arrangements, including Work from Home (WFH) or remote operations, where feasible
- Periodically review preparedness based on organizational and external changes

d. Policy Review and Continuous Improvement

This policy shall be:

- Reviewed periodically or following major disruptions
- Updated to reflect changes in operations, risks, or structure
- Approved by top management and communicated across the organization

Signed by **Chairman & MD** Effective Date: 18th Dec 2025



Mr Antony Selvaraj

Annexure A – Business Continuity Plan

As part of NIST Global operations, the following continuity plans shall be adopted and deployed to ensure uninterrupted service delivery during disruptions.

a. Leadership and Workforce Continuity Plan

- **Director Continuity and Delegation:** Assign alternate Director-level authority for approvals, client escalation, accreditation decisions, and financial commitments to ensure uninterrupted governance during prolonged absence.
- **Interim Leadership Activation:** Activate an interim leadership structure with defined escalation paths to manage operations, delivery decisions, and stakeholder communication when multiple Directors are unavailable.
- **Department Backup Coverage:** Maintain designated backups for department-critical roles such as Training Operations, Client Coordination, Accreditation, Audit Delivery, Sales, Finance, and IT to prevent service disruption.
- **Cross-Training and Knowledge Continuity:** Ensure cross-training across departments to enable smooth handover of critical responsibilities and continuity of operations.
- **Bulk Resignation Risk Management:** Maintain continuity during multiple resignations through resource redeployment across centres, backup client coordinators, and planned replacement mechanisms for client-facing roles.

b. B2C Operations

- **Decline in enrolments:** Shift planned ILT batches to online/virtual batches, activate past-lead/learner database re-engagement, and run city/industry targeted campaigns to stabilize monthly batch occupancy.
- **Accreditation risk (non-renewal/suspension):** Maintain a renewal tracker with assigned owners and a centralized evidence file repository, complete internal compliance reviews prior to due dates, and keep alternative international programs available to ensure training continuity in case of any accreditation status impact.
- **Delivery disruption:** Maintain a backup trainer pool and standardized training decks and lesson plans to ensure uninterrupted batch delivery during trainer unavailability.

c. B2B Operations

- **Tight deadlines:** Use resource redeployment across centres, prioritize commitments through delivery calendar control, and activate backup trainers/auditors to avoid slippage in client schedules.
- **Low order inflow:** Maintain continuity via key account pipeline reviews, cross-selling across training/audit/consulting, and active engagement with existing corporate clients for repeat programs.
- **Client coordination risk:** Ensure at least two trained coordinators per key client and maintain centralized client documentation (scope, schedule, approvals, contacts).

d. **B2G Operations**

- **Order delay/suspension**: Reassign deployed teams to B2B/B2C deliveries or internal project work until project restart and maintain formal communication trail with the government stakeholder.
- **Approval/payment dependency:** Maintain project cashflow continuity through billing milestone tracking, defined escalation for pending approvals, and internal working-capital controls during delayed payments.
- **Dependency risk:** Reduce reliance by maintaining parallel opportunities across multiple government departments / regions.

e. Technology, Data, and Information Security Continuity

- **Cybersecurity and Data Protection:** Protect systems (email, cloud storage, LMS/TMS, client files) through role-based access, MFA, endpoint security, device encryption where applicable, and secure backups with restore testing, aligned with ISO/IEC 27001 information security controls.
- **Cyber Incident Response and Recovery:** Ensure continuity during cyber incidents through an established incident reporting channel, immediate system isolation, account access reset, recovery from secure backups, and defined IT ownership with escalation to management
- **Third-Party Service Downtime Management:** Manage third-party cloud downtime through alternate access methods, offline copies of critical delivery materials, and provider escalation as per service agreement.

f. Crisis and Disruption Management

- **For pandemics / movement restrictions**: Activate work from home (WFH) for support functions and shift delivery to online training, remote client coordination, and virtual audits where feasible.
- **For natural disasters/fire/office inaccessibility:** Activate alternate work location / remote operations, secure people first, and resume critical operations using cloud access and backup resources.
- **For travel incidents during audits/inspections:** Activate travel escalation matrix, coordinate immediate support, and replace field resources using standby auditor/trainer availability.

g. Financial and Commercial Resilience

- **Low Business Period Sustainability:** Sustain operations during low business periods through monthly cashflow monitoring, cost prioritization, and continuity buffer planning for essential payroll and critical operations.
- **Competitive Pricing and Revenue Protection:** Manage competitor price pressure through value-based packaging (training + audit + digital add-ons), maintaining service quality and differentiators rather than price-only competition.

- **Continuity Funding and Contingency Readiness:** Maintain continuity funding readiness through approved contingency allocation for critical disruptions.

h. Communication and Reputation Management

- **Disruption Communication Control:** Ensure disruption communication through single approved spokesperson, internal updates to staff, and controlled external updates to clients and stakeholders.
- **Misinformation and Reputation Response:** Manage misinformation/reputation attacks through fact-based official statements, escalation to leadership, and documented responses through approved channels only.
- **Client Confidence and Service Continuity Updates:** Maintain client confidence by issuing timely service impact updates and revised delivery plan for affected batches/projects.