Business Continuity Plan

Owner: Business Continuity Plan

Date: 27/07/2025

Version: 2

Juniper Education

Juniper Education
Boundary House, 4 County Place
Chelmsford,
Essex, CM2 ORE

Contents

Business Continuity Plan

1. Objectives

1.1 The objective of this Business Continuity Plan (BCP) is to ensure that Juniper Education can continue critical business operations with minimal disruption in the event of a crisis. This includes incidents affecting systems, people, facilities, or third-party services. This draft is being prepared during the current Business Impact Assessment (BIA) process to provide interim continuity assurance to stakeholders and clients.

2. Scope

2.1 This BCP covers all departments and critical systems identified in the ongoing BIA process. This includes but is not limited to:

- Finance (Reporting, Core, Credit Control, Order Desk, Data Intelligence)
- Sales and Marketing
- Customer Support and Success
- DevOps, IT Infrastructure, and Engineering
- HR, Payroll, Legal, Product, Training Services

3. Roles and Responsibilities

- Executive Sponsor (Chief Financial Officer) – Senior financial leader responsible for endorsing, funding, and overseeing the BCP across the organisation.
- Business Continuity Managers (GISO, GDPO, GITM) - Key leads responsible for developing, coordinating, and maintaining the BCP, each with focus on governance, data protection, and technology continuity.
- Department heads – Managers who ensure departmental preparedness and adherence to the BCP.
- IT Team – Technical team managing infrastructure resilience, recovery, and system access.
- HR - Team responsible for staff communication, availability, and contact accuracy.
- All Staff - Employees who must understand and follow their role in the BCP process.

4. Definitions

- **BCP – Business Continuity Plan** - A structured and documented strategy that outlines how an organisation will continue to operate during and after an unplanned disruption or crisis. The BCP details procedures for maintaining essential functions, protecting assets, minimising downtime, and ensuring a timely recovery of critical business processes.
- **BIA – Business Impact Assessment** - A systematic process used to evaluate and identify the potential effects of disruptions on business operations. It assesses the criticality of departments, systems, and processes, and helps prioritise recovery strategies based on their operational and financial impact.

- **RTO – Recovery Time Objective** - The maximum acceptable amount of time that a system, application, or process can be unavailable after a disruption before significantly impacting the organisation. It guides the development of recovery strategies and determines urgency for response efforts.
- **RPO – Recovery Point Objective** - The maximum amount of data loss (measured in time) that an organisation can tolerate during a disruption. It defines the frequency of data backups and determines how current the restored data should be after recovery.
- **Critical System** - Any system, platform, or service that is essential for the continuity of operations. Failure or unavailability of a critical system would cause severe disruption to business functions, regulatory compliance, customer delivery, or financial performance. These systems typically require the highest priority in recovery planning.

5. Associated Documents

- Business Impact Assessment (BIA)
- Disaster Recovery Plan – Under development
- Communications Plan
- Risk Register
- Vendor Support Agreements

6. Testing

6.1 Regular testing will be conducted annually or after a major change or event, covering:

- System failover drills
- Staff remote access readiness
- Communication validation
- Department-specific recovery simulations

7. Storage

7.1 This BCP will be stored:

- Electronically in a secure SharePoint repository
- Offline on encrypted removable drives (IT-managed)
- Printed copies held by Department Heads and Executive Team

8. Priorities

8.1 Prioritisation is based on current BIA outputs:

8.1.1 Tier 1: Critical (RTO < 4 hours)

- Payroll
- Finance Systems
- Microsoft Office 365
- Code repositories
- Backup & Recovery
- DevOps/Engineering Tools

8.1.2 Tier 2: High (RTO < 24 hours)

- CRM
- Communication Tools
- Customer Service Systems
- Marketing Automations

8.1.3 Tier 3: Medium (RTO 2–5 days)

- Training Systems
- Reporting tools
- HR/Recruitment Platforms

9. Business Continuity Team

Role	Responsibility
CFO	Executive Sponsor
Head of Data Security & Compliance GISO GITM	Business Continuity Manager(s)
GITM	IT Manager (Lead)
CHRO	(HR Lead)
CTO	Products & Engineering Lead
CHRO - Staff communications Head of Operations Software (Customer Support) - Customer communications	Communications Lead
Finance (Reporting) – CFO Finance (Core) – Group Financial Controller Finance (Credit Control) – Credit Control, Contracts & Compliance Manager Finance (Order Desk) – ERP & CRM Finance Manager Finance (Data Intelligence) – Head of Revenue and Growth Finance (Security & Compliance) – Head of Data Security & Compliance IT & Infrastructure – GITM HR – CHRO Payroll - CHRO Sales – Head of Sales Marketing – Head of Marketing Customer Support – Head of Operations Software (Customer Support) Customer Success – Head of Customer Success	Department Head Representatives as needed

Juniper Training Services – Training & Development Manager Dev Ops – Lead DevOps Engineer SLT – CEO Engineering – Director of Engineering Product – CTO Facilities – Facilities Manager	

10. Business Continuity Management Centres

10.1 Contingency Office Location & Remote Operations

10.1.1 In the event of a site-wide disruption, Juniper Education will transition to fully remote operations. All staff are equipped to work from home using secure VPN connections and cloud-based systems. Critical tools are accessible remotely with multi-factor authentication and endpoint security in place.

10.1.2 Preconfigured devices, secure access protocols, and collaboration tools ensure business continuity across all departments. The Business Continuity Team will oversee operations, and Department Heads will manage their teams remotely until normal office access is restored.

11. BIA Summary / Analysis

11.1 The Business Impact Assessment (BIA) has highlighted the following critical dependencies and operational risks:

- **Payroll and Finance Operations**
  Disruptions to core finance systems can severely affect compliance, financial reporting, and employee payment processes in less than 24 hours. These functions are time-sensitive and require immediate restoration to avoid operational and legal consequences.

- **DevOps Toolchain**
  The software development and infrastructure environments are vital for product deployment, version control, and ongoing support. Any prolonged outages could compromise service delivery and customer commitments.
- **Primary Communication and Collaboration Tools**
  The loss of access to primary communication and collaboration tools would significantly impair both internal coordination and external communications.
- **Systems Without Practical Workarounds**
  Several systems do not have practical or sustainable fallback options. While some manual workarounds exist**,** they are highly labor-intensive and inefficient**,** especially over extended periods. Even where a workaround is technically feasible, it would place significant strain on resources and staff capacity. Prolonged outages in these tools even if not top-tier critical, can still disrupt workflows and impact delivery timelines.

12. Thresholds and Contingency Plans

12.1 As part of Juniper Education's continuity planning, thresholds have been established to categorise the severity of business disruptions based on duration and operational impact. These thresholds guide the response strategy and escalation procedures depending on how long a function, system, or facility remains unavailable.

Impact Window	Impact level	Response strategy
0-1 days	High	Within the first 24 hours, failover systems or manual workarounds are activated to maintain critical services. Department heads initiate contingency steps while the Business Continuity Team monitors impact.
2-10 days	Catastrophic	Disruptions over one day trigger emergency recovery, including IT disaster plans and vendor escalation. Priority is placed on restoring services via backups or alternate resources.
10-30 days	Catastrophic	After 10 days, a full restoration strategy begins, including staff redeployment and workload shifts. Clients are updated, and the Executive Team oversees key decisions with department leads.
>30 days	Catastrophic	Disruptions over 30 days prompt strategic action by the Executive Team, including reviewing contracts, adjusting operations, and exploring long-term support or delivery changes.

13. BCP and Critical Contacts

13.1 To ensure effective execution during a disruption, copies of the Business Continuity Plan (BCP) and clearly defined escalation paths will be distributed to key internal and external stakeholders. This will enable timely action, cross-functional coordination, and compliance with client and vendor expectations.

13.2 BCP Access and Distribution

13.2.1 The BCP is actively shared with the following roles and teams:

- **Executive Team**: Responsible for strategic oversight, decision-making, and overall coordination during a major incident.
- **Department Heads**: Accountable for executing continuity procedures within their functional areas and ensuring team readiness.
- **Client Service Leads**: Ensure that client-facing communications and service-level expectations are maintained.

- **Key Vendors and Third Parties**: Especially those with active Service Level Agreements (SLAs) that reference or require business continuity capabilities, such as hosting providers, security partners, and system integrators.

13.3 Critical Contacts List

13.3.1 A centralised Critical Contacts List will be maintained within the Juniper's internal SharePoint repository**.** This list will be regularly reviewed and updated to ensure accuracy and rapid access during an incident. It includes:

- **External IT Providers**: Key partners responsible for hosting, infrastructure, backups, and cloud services.
- **Emergency Response Services**: Relevant local authorities and emergency contacts, including law enforcement, medical, or facility management responders.
- **Client Stakeholders**: Designated contacts at client organisations who require timely updates, especially in the event of service disruption or risk to contract deliverables.

Date	Policy Owner/Author	Version	Reason for Change	Approved by	Review Date
26/09/2025	GISO	2	Published	Head of Data Security & Compliance	28/09/2026

Juniper Education

We look after you, so that you can look after our children

Juniperеducation.org