Business Continuity Plan

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

I. Purpose

This plan aims to minimize interruptions to normal operations, limit the extent of disruptions and damage in disasters, and establish alternative means of operation in the event of emergencies.

II. Scope

Disruptions include product outages, internet outages, economic disruption, loss of key personnel, cyberattacks, and negative publicity. This policy affects all employees of this Nested Knowledge and its subsidiaries, and all contractors, consultants, temporary employees and business partners.

III. Business Continuity Plan

The following covers the types of disruptions planned for, the roles of key personnel in continuity planning and disruption response, the applications that could be disrupted, and the general strategies for ensuring business continuity.

Examples of Disruptions

- External Product outage
- File Share goes down
- Unplanned internet outage
- Data loss
- Hardware/software failures
- Economic disruption
- Recession
- Turnover of critical employees
- Cyberattacks
- Negative Publicity (Reputation)

Application Profile

Name	Manufacturer	Critical to Business?	Critical to application?	Comments
AWS	Amazon	Yes	Yes	Essential for running AutoLit/Synthesis

Name	Manufacturer	Critical to Business?	Critical to application?	Comments
NPM	Microsoft	Yes	Yes	Essential for building production deployments. In the event of repository outage, dependencies may be transferred from backups via FTP.
PyPi		Yes	Yes	Essential for building production deployments. In the event of repository outage, dependencies may be transferred from backups via FTP.
Auth0		Yes	Yes	Essential for providing authorization & username/password management to all users.
Stripe		No	No	Stripe enables pay-on-the-site. Both paying and non-paying users may continue accessing the site in the event of an outage, and payments & subscriptions may be manually managed by the NK team in the event of a long-term outage.
Google Suite	Google	Yes	No	In the event of an email disruption, we will shift to Outlook-based or other email platforms. In the event of a disruption to Google Meets, we will utilize Zoom for video calls. In the event of a document storage disruption, we will utilize Box for storing company documents.
Toggl	Toggl	No	No	Used for employee and contractor time tracking. If a disruption occurs, we will require manual time tracking
Gusto		Yes	No	Essential for payroll and benefits.
QuickBooks		Yes	No	Essential for storing financial information.
Slack		No	No	Utilized for business communication. If a significant disruption occurs, we will switch instant messaging to the chat application Signal.
GitLab		Yes	Yes	If a temporary disruption occurs, we will employ FTP & patch files.
Carta		No	No	
Pubmed Entrez API		No	No	When a disruption occurs, manual and recurrng searches fail. Upon recovery, our system automatically begins rerunnning scheduled failed searches.
Unpaywall		No	No	When a disruption occurs, the full text import feature is shown as “Not Available” on site.
HubSpot		No	No	
Adobe Creative Cloud		Yes	No	(Photoshop, Illustrator, InDesign, After Effects, Premiere Pro)

Name	Manufacturer	Critical to Business?	Critical to application?	Comments
Adobe Reader		No	No	In the event of a disruption to Adobe Reader, we will switch to Docusign.
OBS Studio		No	No	
Metabase		No	No	Include sensitive and confidential data.
Scite		Yes	Yes	When a disruption occurs, the scite badge no longer displays.
ClinicalTrials.gov		Yes	Yes	When a disruption occurs, manual and recurring searches fail, and NCTID bibliomining will fail. Upon recovery, our system automatically begins rerunnning scheduled failed searches.
EuropePMC		Yes	Yes	When a disruption occurs, manual and recurring searches fail. Upon recovery, our system automatically begins rerunnning scheduled failed searches.
DOAJ		Yes	Yes	When a disruption occurs, manual and recurring searches fail. Upon recovery, our system automatically begins rerunnning scheduled failed searches.

Roles and Contacts

Name	Title	Role/Function	Contact Information
Kevin Kallmes	CEO	Executive decisions; personnel management	kevinkallmes@supedit.com 507-271-7051
Karl Holub	CTO	Technical Lead	karl.holub@nested-knowledge.com
Kathryn Cowie	COO	Operational support	kathryn.cowie@nested-knowledge.com 301-272-0957

Business Continuity Strategies

Loss of Function of Critical Applications

- In the case of the loss of functionality to AutoLit or Synthesis for at 30 or more minutes, the CTO will be notified and we will send out a Site Disruption message to all users. The CTO and development team will assess the extent of any lost capabilities and timeline to restoration, and then communicate with company leadership regarding a recovery plan of specific functions.
- In the case of the loss of functionality to any other key/critical applications, the CTO will be notified; Site Disruption messages will only be sent to users in the case that this impacts end user functions. In consultation with company leadership, the CTO and development team will create a plan to either restore function or shift to a different software provider.
- In case of outages, the CEO or another leader will email account representatives for customers with a proposed restoration timeline and details regarding the outage.

Recession Planning

- Our finances are based on private funding and revenue. Our costs are based on already-negotiated contracts with employees and contractors. We would be open to federal support (such as the Payroll Protection Plan) or bank loans, but should not need to dramatically alter financing in a recession.

Loss of Key Personnel

- In the event that Nested Knowledge loses our CTO, we will elevate our head engineer to replace the duties and hire an additional engineer as soon as feasible.
- In the event that Nested Knowledge loses our COO, we will hire an already trained Operations Manager and Bookkeeper to aid with record keeping and financial operations.

Compliance Statement

All Employees and Contractors who access Nested Knowledge's information systems will be provided with and required to review this document. Personnel with central roles in business continuity planning will undergo annual training to ensure competence with business continuity procedures.

Business Impact Analysis (BIA)

I. Purpose

The goal of the BIA is to provide a framework for evaluating business activities and their associated resource requirements to determine how critical they are for business operations. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives.

II. Scope

This plan applies to Nested Knowledge employees and contractors.

III. BIA Plan

The BIA is composed of:

i) Criticality

Identify the impact of a system disruption to critical business processes

ii) Resources

Determine resources required to resume business processes as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

iii) Priorities

Establish priority levels for recovery activities and resources.

Updating and Review

The BIA should:

- Undergo scheduled review for applicability and appropriate criticality, resourcing, and prioritization.
- Unless determined otherwise, the BIA will be reviewed annually, starting in 2022.
- Undergo changes with major changes to the business or its products, including but not limited to the launch of a new software product, an integration with an existing software product, or the creation of any new services based on the product.
- Undergo changes with major changes to the ownership or oversight, including but not limited to acquisition, joint venture, or transfer of 51% of the voting shares in the company.

Estimating Downtime

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Resource	RTO	RPO	Comments
Application Code (sitewide functionality outage)	30 minutes	N/A	Bugs are most likely to be caught in verification immediately after deployment (15 minutes). In this event, the release is rolled back (5 minutes) and additonal time provided for any database schema rollbacks (10 minutes).
Critical Databases	15 minutes	5 minutes	Transaction logs are streamed to a backup on AWS RDS. A new instance may be provisioned from an arbitrary timepont (10 minutes) and the private DNS record updated (5 minutes).
Critical Servers	30 minutes	N/A	New compute images have a scripted provisioning (15 minutes) and run a deploy inside 10 minutes.

Resource	RTO	RPO	Comments
AWS (permanent outage)	40 hours	12 hours	This entry highlights a worst-case scenario: a permanent AWS outage requiring transfer of our services to a different cloud services provider (planned: Google Cloud). Time is alloted for provisioning of compute, load balancing, & database resources, transfer of database backups, DNS record transfer (or temporary new record creation), network configuration. Database backups are performed twice daily to an offsite, giving an RPO of 12 hours.
AWS (transient outages)			We defer to AWS's SLAs for service outages that do not require as serious action as a full transfer away. Services relevant to NK are Compute (servers), Databases, and Networking and Content Delivery (VPC, firewall, DNS).

Maximum Tolerable Downtime (MTD):

For any cause: 48 hours. This estimate represents the RTO for a worst-case failure (permanent outage & transfer off of our current cloud provider), plus an 8 hour Work Recovery Time (WRT) verifying the new system.

Business Impact Analysis Schedule:

Nested Knowledge will perform a Business Impact Analysis on an annual basis, beginning in the first quarter of 2022.

Disaster Planning and Recovery

I. Purpose

This document explains Nested Knowledge's procedure for mitigating disruption of product and services delivery when disruption due to disaster occurs. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

II. Scope

This policy affects all employees and contractors of Nested Knowledge.

III. Disaster Plan

Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential Disaster	Likelihood	Consequence	Remedial Actions
Pandemic	Highly Possible	Minor	No onsite location at risk; we will continue to build products and provide services in pandemics.
Act of Terrorism	Possible	Minor	No onsite location at risk; however, a terrorist attack may disrupt personnel hours and availability or impact data centers. This risk is managed by AWS.
Fire	Unlikely	Minor	No onsite location at risk; however, a fire may disrupt personnel hours and availability or impact data centers. This risk is managed by AWS.
Tornado	Unlikely	Minor	No onsite location at risk; however, a tornado may disrupt personnel hours and availability or impact data centers. This risk is managed by AWS.
Disruption of servers	Unlikely	Major	This risk is managed by AWS. We operate out of multiple availability zones to increase resiliency to a single data center outage.

Emergency and Disaster Recovery Team

The disaster recovery team consists of Kevin Kallmes, Karl Holub, Kathryn Cowie. In the event of an emergency, the team's responsibilities include:

- Respond immediately to a potential disaster and call emergency services
- Assess the extent of the disaster and its impact on the business.
- Notify employees and allocate responsibilities and activities as required
- Restore critical services within four business hours of the incident.
- Recover to business as usual within 8 to 24 hours after the incident

Communication and Notifications

Notification of Emergency

The person discovering the incident should call or email a member of the Emergency and Disaster Recovery Team immediately.

Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff are advised to call the staff member's emergency contact to relay information on the disaster.

Personnel/Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

Media Contact

If applicable, assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

Insurance Requirements

As a mitigation of financial risk, legal exposure, data privacy breach, and other key company functions, the company will maintain the following insurance policies:

- General Business / Professional Liability Insurance
- Network Security and Privacy Liability Insurance
- Cyber Crime Insurance
- System Damage and Business Interruption Insurance

Finances and Legal Action

Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability

- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post- disaster.

Legal Actions

The company lawyer and Emergency and Disaster Response Team will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

Tabletop Exercises

On an annual basis, the executive and engineering management teams will independently develop a set of 10 potential disruptive and disaster scenarios to our product, resources, and external dependencies. 5 scenarios will be randomly selected with the scenario moderator acting as moderator for each exercise. The moderator will accept planned actions & team-level assignments and return outcomes, optionally adding in modifying information or new developments.

Scenarios are carried forward year to year.

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	11/15/2021	In progress; application profile and risk register need technical review.
K. Kallmes	11/19/2021	2021 version finalized and signed off
K. Holub	06/25/2022	Added a new supplier
P. Olaniran	10/24/2022	Reviewed w/ Kevin K., Karl H., Kathryn C.
K. Kallmes	1/26/2023	Reviewed BIA

Return to Policies