BUSINESS CONTINUITY PLAN

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

Business Continuity Plan
Version 1.0
January 1, 2021

NextGen CGI, LLC							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Purpose

Business continuity and disaster recovery plans are intended to provide step-by-step procedures for establishing reliable, continuous business operations and recovering from disrupted systems and networks associated with the organization. The goal of these processes is to minimize any negative impacts to company operations. This process identifies critical IT systems and networks, prioritizes recovery time objectives (RTOs), and delineates the steps needed to restart, reconfigure, and recover from them. This plan also includes all relevant internal and external contacts that are involved on the business continuity and disaster recovery process.

2. Scope

This policy applies to all company officers, directors, IT support specialists, agents, affiliates, contractors, consultants, advisors or service providers that are involved in the business continuity and disaster recovery process at NextGen CGI. It is the responsibility of all the above to familiarize themselves with this policy and ensure adequate compliance with it. All systems connected to the network should be considered and included in the business continuity and disaster recovery process.

3. Business Continuity Policy

This policy is designed to respond to a significant business disruption (SBD) by safeguarding IT support specialist's lives and company property, perform financial and operational assessments, recover and resume operations, protect all data, and allow customers to continue to utilize services and transact with the business. In the event that the organization is unable to continue business operations, all customers and partners will be promptly notified.

3.1 Significant Business Disruptions (SBDs)

3.1.1 The plan anticipates two kinds of SBDs – internal and external. Internal SBDs affect only the organization's ability to communicate and do business, such as a fire in the data center. External SBDs prevent the operation of service providers, logistics, supply chains, and other organizations or processes that are involved in usual business operations such as a terrorist attack, a city flood, or a wide-scale, regional disruption. Our response to an external SBD relies more heavily on other organizations and systems.

3.2 Approval and Execution Authority

3.2.1 Stacy Hall is responsible for approving the plan and conducting the required annual review process.

3.3 Plan Location and Access

3.3.1 The organization will maintain copies of the business continuity plan (BCP), annual reviews, and changes that have been made to it. An electronic copy of the plan is located here: https://nextgencgi.com/pdf/Business-Continuity-Plan.pdf

4. Succession Planning

If the assignee outlined in section 3.2 becomes incapacitated or unavailable, all business operations fall to the secondary assignee: Benjamin Estes. If the secondary assignee becomes unavailable, all business operations will fall to the tertiary assignee: Daniel Hanic.

5. Office Locations

The company is located at the address(es) listed below. IT support specialists may travel to this location by various modes of transport.

- 6033 Castlegate Dr W Ste 2715, Castle Rock, Colorado 80108 (USA)

NextGen CGI engages in the following mission critical systems at these locations:

- Cloud migration processes on the Ionos 1&1 infrastructure

6. Alternate Physical Location(s) of IT support specialists

In the event of an internal SBD that precludes the use of the primary office location(s), all staff will be moved from affected offices to each staff member's respective home to work remotely. The main contacts will be the personnel outlined in Section 4, and a mass-distributed email will be distributed to all staff via electronic communication.

7. Data Backup and Recovery

NextGen CGI maintains its primary records and data at the below address.

- 6033 Castlegate Dr W Ste 2715, Castle Rock, Colorado 80108 (USA)

Stacy Hall is responsible for the maintenance of this information. This data includes, but is not limited to, the following document types and forms:

- See policy index (https://nextgencgi.com/?p=info.cybersecurity)

Electronic record backup, to include offsite backup, are conducted in the following manner and frequency:

- Daily system-wide automated cloud backup
- Local secure data backup and storage

- Secondary secure data backup and storage in undisclosed locates protected by the confidential records maintained by Stacy Hall

In the event of an internal or external SBD that causes the loss of paper records, the organization will physically recover them from the electronic backup repository. If the primary site is inoperable, the organization will continue operations from the alternate location(s) listed in Section 6, until such time that an alternate primary site has been secured.

8. Operational Assessments

In the event of an SBD, the organization will identify what means will permit communication with clients, IT support specialists, partners, and stakeholders doing business with the organization. Although the effects of an SBD will determine the means of alternative communication, the communications options that will be employed include the website, telephone, voice mail, and e-mail. In addition, the organization will retrieve key activity records as described in Section 7.

9. Mission Critical Systems

The organization's mission critical systems are those that ensure prompt and accurate processing of data for customers, to include the following:

- Internal computer network and terminal access devices
- Local and remote data backup systems
- Network connection
- Realtime systems and network monitoring
- Maintenance of confidential information
- Maintenance and protection of client personal details
- Maintenance and protection of business records

The organization has primary responsibility for establishing and maintaining business relationships with customers and stakeholders and has sole responsibility for the mission critical functions outlined above.

Recovery Time Objectives (RTOs) provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency, and various external factors surrounding disruption, such as time of day, scope of disruption, and status of critical infrastructure, can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption. The organization makes every best effort to mitigate reasonable risk of service interruption, and in the event of an SBD, the recovery time and resumption objectives are to resume regular business as soon as possible given

the implementation of geographically diverse service centers allowing rapid transfer of work to alternate locations.

Below is a summary of each mission critical system outlined above, and the continuity/response plan that will be executed if the system becomes inoperable or disrupted:

- The summary of mission critical systems and response plan for each system is CONFIDENTIAL

10. Alternate Communications with Stakeholders

10.1 Customers

The organization communicates with customers using telephone, email, US mail, and in-person visits. In the event of an SBD, an assessment will be conducted to determine which means of communication are still available, after which the fastest method will be employed to communicate with customers and partners alike.

10.2 IT support specialists

The organization communicates with IT support specialists using telephone, email, and in person. In the event of an SBD an assessment will be conducted to determine which means of communication are still available, after which the fastest method will be employed to communicate with IT support specialists. The organization will also employ a call tree so that senior management can reach all IT support specialists quickly during an SBD. The call tree will include all staff home and office phone numbers. The personnel authorized to invoke the call tree are outlined in Section 4.

10.3 Partners and Third Parties

The organization communicates with partners and third parties using telephone, email, US mail, and in-person visits. In the event of an SBD, an assessment will be conducted to determine which means of communication are still available, after which the fastest method will be employed to communicate with partners and third parties.

11. Critical Business Constituents and Third Parties

The organization has contacted all critical business constituents (businesses with which the organization has ongoing commercial relationships in support of operating activities) and determined the extent to which relationships can be continued in the event of internal or external SBDs. The organization will quickly establish alternate arrangements

if a business constituent can no longer provide the needed services or goods. Below is a list of all business constituents and contact information in the event of an SBD:

- Ionos 1&1 - https://contact.ionos.com/contact

12. Related Standards, Policies, and Processes

- Incident Response Policy
- Disaster Recovery Plan
- Vendor Management Policy
- Change Management Policy

13. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

Term	Definition
RESERVED	RESERVED