The NoCheck Group, LLC (NoCheck)
Business Continuity/Contingency Plan (BCCP) 2021

Background

This document has been developed for mission-critical business processes and works in conjunction with NoCheck's DRP.

What is Contingency Planning?

Contingency Planning is a process that develops alternative, or contingent, business process plans to continue with mission-critical business processes after their standard means of operation have been interrupted, preventing execution of the primary mission-critical business processes. In short, it is insurance against disaster.

How Does Contingency Planning Relate to Business Process Risk?

Contingency Plans are developed to create an alternative to the primary mission-critical business process. They differ from mitigation plans in two ways: first, contingency plans are developed to temporarily replace a business process; and second, they are enacted following the incidence of business process interruption.

Why am I Developing a Contingency Plan?

It is imperative that The NoCheck Group institute alternative or contingent, business process plans to continue with mission-critical business processes and ensure continuity of services following interruption of the primary mission-critical business processes.

I. Emergency Contact Persons

Our firm's three emergency contact persons are:

Chuck Kopko, President, Cell #248-973-7291
Don Artman, Vice President, Operations Manager, Cell #734-431-3302
Mike Elliott, Network Engineer, Cell # (248) 842-5144

II. Firm Policy

Our firm's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of the firm's books and records, and allowing our customers to transact business.

A. Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building. External SBDs prevent the operation of services; such as a terrorist attack, a city flood, or a wide-scale, regional disruption.

B. Approval and Execution Authority

Chuck Kopko, President of NoCheck, a registered principal, is responsible for approving the plan and for conducting the required annual review. Don Artman, Vice President, Operations Manager has the authority to execute this BCP.

C. Plan Location and Access

Our firm will maintain copies of its BCP plan and the annual reviews, and the changes that have been made to it for inspection. An electronic copy of our plan is located on our shared drive (S:\Office\NoCheck Group Policy & Procedures).

III. Business Description

Our company conducts business in software development, application service provider and enrollment processes for financial processing. We also provide customer service processes for our clients. All transactions are sent to our banking partner, JP Morgan Chase.

IV. Office Locations

The NoCheck Group, LLC (NoCheck) has offices located in Southfield, MI and Grand Rapids, MI.

A. Office Location #1

Our Location #1 Office is located at 24400 Northwestern Hwy, Suite 221/220, Southfield, MI 48075. Its main telephone number is 248-228-8700.

B. Office Location #2

Our Location #2 Office is located at 3950 Sparks Dr., Grand Rapids, MI 49546. Only hardware and software reside at this location, no staff is permanently located here.

C. Office Location #3

Location #3 is located in Luxembourg, at EBRC, 5, Rue Eugene Ruppert, L-2453 Only hardware and software reside at this location, no staff is permanently located here.

V. Alternative Physical Location(s) of Employees

In the event of a disaster, we will move our staff from affected office location #1 to the offices of location #2.

VI. Customers' Access to Data

The NoCheck Group has redundant connections to the internet at all three locations, we have redundant servers for all our clients, and we have redundant generator backups at all three locations. We also maintain backups of all data and servers on-site and off-site.

Critical Elements

There are 10 critical elements of a BCP.

(1) Data back-up and recovery
(2) All mission critical systems;
(3) Financial and operational assessments;
(4) Alternate communications between customers and the member;
(5) Alternate communications between the member and its employees;
(6) Alternate physical location of employees;
(7) Critical business constituent, bank, and counter-party impact;
(8) Communications with regulators; and
(9) How The NoCheck Group, LLC will assure customers' access to their data.

VII. Data Back-Up and Recovery

Our firm maintains its primary data backup on-site and off-site. Our first line of defense is we have backup servers in two locations, one backup server at site location #1 and a second backup server located at site #2. We also maintain data backups at site location #1 and off-site located in a safety deposit box and Chase Bank. We also maintain our accounting records on-site and off-site. Chuck Kopko is responsible for maintaining the accounting records and Don Artman's team is responsible for maintaining the data backups. The NoCheck Group backs up its electronic records daily.

In the event of an internal or external disaster that causes the loss of our electronic or paper records, we will physically recover them from our back-up site. If our primary site is inoperable, we will continue operations from our back-up site (Location #2 & #3). For the loss of electronic records, we will either physically recover the storage media or electronically recover data from our back-up site, or, if our primary site is inoperable, continue operations from our back-up site (Location #2 & #3).

VIII. Financial and Operational Assessments

A. Operational Risk

In the event of a disaster, we will immediately identify what means will permit us to communicate with our customers, employees, critical business constituents, critical banks and critical counter-parties. Although the effects of a disaster will determine the means of alternative communication, the communications options we will employ will include our website, telephone voicemail, cell phones and email. In addition, we will retrieve our key activity records as described in the section above, Data Back-Up and Recovery.

B. Financial and Credit Risk

In the event of a disaster, we will determine the value and liquidity of our assets to evaluate our ability to continue to fund our operations and remain in compliance. We will contact our critical banks and owners to apprise them of our financial status. If we determine that we may be unable to meet our obligations to those counter-parties or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations to our clients.

IX. Mission Critical Systems

Our firm's "mission critical systems" are those that ensure prompt and accurate processing of data for our clients, including enrollment taking, entry, data file transfers and transactions, the maintenance of customer web sites and data, access to web sites and customer service.

We have primary responsibility for establishing and maintaining our business relationships with our customers and have sole responsibility for our mission critical functions of enrollment processing and file transmissions to our banking partners.

A. Our Firm's Mission Critical Systems

1. Enrollment collection through the internet, fax, telephone and US Mail

Currently, our firm receives enrollments from our client's customers via the internet, fax, telephone and US Mail. During a disaster, either internal or external, we will continue to receive enrollments through our redundant web servers, fax, email and telephone by utilizing our backup site located in Grand Rapids, MI.

X. Alternate Communications between the Firm and Customers, Employees, and Regulators

A. Customers

We now communicate with our customers using email, telephone, website, and US mail and in-person communication. In the event of a disaster, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with our clients and partners. For example, if we have communicated with a party by email but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail.

B. Employees

We now communicate with our employees using email, telephone, website, and US mail and in-person communication. In the event of a disaster, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with our employees. For example, if we have communicated with our employees by email but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail. We have identified persons, noted below, who live near each other and may reach each other in person:

The person to invoke the use of the call tree is: Don Artman, V.P., Operations Manager

Caller	Call Recipients
Don Artman	*Chuck Kopko, Jim Hoxsey*
	Mike Elliott

XI. Critical Business Constituents, Banks, and Counter-Parties

A. Business constituents

We have contacted our critical business constituents (businesses with which we have an ongoing commercial relationship in support of our operating activities, such as vendors providing us critical services), and determined the extent to which we can continue our business relationship with them in light of the internal or external disaster. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of a disaster to them or our firm. Or, we have entered into a supplemental contract with certain critical business constituents to provide such services. The alternative suppliers are disclosed below. Our major suppliers are:

AT&T, 16025 Northland Dr, Suite 300, Southfield, MI 48075
M: 248-205-9708
Primary fiber connection

Everstream, 3950 Sparks Dr., Grand Rapids, MI 49546
586- 873-4434
Co-Location partner, secondary fiber connection

123.net, Northwestern Hwy, Southfield, MI
Phone system

JP Morgan Chase
Tampa, FL
Data processing

B. Banks

We will contact JP Morgan Chase and Key Bank to determine if they can continue to provide the data processing of files for our clients.

XII. Disclosure of Business Continuity Plan

Attached is our written BCP plan we provide customers at account opening and annually if changes have been made. We also mail it to customers upon request.

XIII. Updates and Annual Review

The NoCheck Group will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm. In addition, our firm will review this BCP annually, in December, to modify it for any changes in our operations, structure, business or location.

XIV. Senior Manager Approval

I have approved this Business Continuity Plan as reasonably designed to enable our firm to meet its obligations to customers in the event of an SBD.

Signed: _____

Title: _____

Date: _____

Attachment A to the NoCheck Group, LLC Business Continuity Plan

The NoCheck Group's Business Continuity Planning

The NoCheck Group, LLC (NoCheck) has developed a Business Continuity Plan on how we will respond to events that significantly disrupt our business. Since the timing and impact of disasters and disruptions is unpredictable, we will have to be flexible in responding to actual events as they occur. With that in mind, we are providing you with this information on our business continuity plan.

Contacting Us – If after a significant business disruption you cannot contact us as you usually do at 248-228-8700, you should call our alternative number 248-973-7291 or go to our website at www.nocheck.com. If you cannot access us through either of those means, you should contact us at another alternative number, 734-431-3302.

Our Business Continuity Plan – We plan to quickly recover and resume business operations after a significant business disruption and respond by safeguarding our employees and property, making a financial and operational assessment, protecting the firm's books and records, and allowing our customers to transact business. In short, our business continuity plan is designed to permit our firm to resume operations as quickly as possible, given the scope and severity of the significant business disruption.

Our business continuity plan addresses: data backup and recovery; all mission critical systems; financial and operational assessments; alternative communications with customers and employees; alternate physical location of employees; critical supplier, contractor, bank and counter-party impact; and assuring our customers prompt access to their data if we are unable to continue our business.

While every emergency situation poses unique problems based on external factors, such as time of day and the severity of the disruption, we are advising that our firm's objective is to restore its own operations and be able to complete existing transactions and accept new transactions within 24 hours

Varying Disruptions – Significant business disruptions can vary in their scope, such as only our firm, a single building housing our firm, the business district where our firm is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only our firm or a building housing our firm, we will transfer our operations to a backup site when needed and expect to recover and resume business within 24 hours. In a disruption affecting our business district, city, or region, we will transfer our operations to a site outside of the affected area, and recover and resume business within 24 hours. In either situation, we plan to continue in business, transfer operations to our backup site if necessary, and notify you through our website www.nocheck.com or our customer emergency number, 248-973-7291 how to contact us. If the significant business disruption is so severe that it prevents us from remaining in business, we will assure our customer's prompt access to their data.