

	Doc Title: <i>NeuStar Business Continuity Plan</i>	
	Doc Number: NEU-00001	
	Doc Revision: 2.4	

Revision Control

Revision	Release Date	Author	Description of Changes
1.0		Security-Related Information	Initial Release
2.0		Security-Related Information	Updated to reflect separation of the Plan and Runbook
2.1		Security-Related Information	Updated to reflect edits
2.2		Security-Related Information	Updated to reflect edits
2.3		Security-Related Info	Updated to reflect edits
2.4	6/18/2012	Security-Related Info	Updated Security-Related Information

Document Approvals of Current Revision

Name:	Position/Title/Role
Alex Tulchinsky	Senior Vice-President of Operations (Or Designate)

Send all Questions, Suggestions and Recommendations regarding the content of this document to

The information contained herein is proprietary to NeuStar, Inc. Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited. Limit distribution accordingly.
 The names, logos, and taglines identifying NeuStar's products and services are proprietary marks of NeuStar, Inc. All other trademarks and service marks are the property of their respective owners. © NeuStar, Inc. 1999-2013

Table of Contents

1	Introduction	5
1.1	Purpose and Scope.....	5
1.2	Assumptions	5
1.3	Plan Development	5
1.4	Plan Maintenance.....	6
1.5	Plan Testing.....	6
2	Assessing Business Risk and Impact of Potential Emergencies	6
2.1	Emergency Incident Assessment	6
2.1.1	Environmental Disasters	7
2.1.2	Security-Related Information	10
2.1.3	Security-Related Information.....	11
2.1.4	Security-Related Information.....	12
2.1.5	Security-Related Information	13
2.1.6	Pandemic	14
2.1.7	Loss of Key Personnel	15
2.2	Business Risk Assessment.....	15
2.3	Business Impact Analysis (BIA)	15
2.4	Critical Business Functions and Recovery Time Objectives (RTO).....	15
3	Recovery and Restoration Planning	18
3.1	Recovery Phase.....	18
3.2	Restoration Phase	18
4	NeuStar Communications Options	18
4.1	Telephone (Landline).....	18
4.2	Telephone (Mobile) or SMS	18
4.3	E-mail.....	19
4.4	IM	19
4.5	GETS, WPS and TSP	19
4.5.1	GETS – Government Emergency Telecommunication Service	20
4.5.2	WPS – Wireless Priority Service.....	20
4.5.3	TSP – Telecommunications Service Priority	20

Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.

5	Security-Related Information	21
5.1	Security-Related Information	21
5.2	Security-Related Information	22
5.3	Security-Related Information	22
	Security-Related Information	22
	Security-Related Information	23
5.4	Security-Related Information	23
5.4.1	Security-Related Information	23
5.4.2	Security-Related Information	23
5.4.3	Security-Related Information	24
5.4.4	Security-Related Information	24
5.4.5	Security-Related Information	24
5.4.6	Security-Related Information	24
5.4.7	Security-Related Information	24
	Appendix A – NPAC Contractual Obligations	26
(a)	Loss of NPAC/SMS Production Computer System site.	26
(b)	Loss of NPAC/SMS Disaster Recovery Computer System site.	26

1 Introduction

1.1 Purpose and Scope

This Business Continuity Plan (aka "the Plan") provides a roadmap to prepare for and respond to a range of potential emergencies/disasters relating to the people, data and facilities that comprise NeuStar's business assets.

The Plan provides a description of the overall disaster/emergency response actions. They designate responsibilities, interface between organizations, and notification procedures necessary to cope with all aspects of disasters.

The Plan identifies the critical functions of NeuStar and the resources required to support them. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and response. Supplementary information, including supporting teams and structures, external first-responder information, and communications resources are documented and maintained in the BCP Supplement.

1.2 Assumptions

The Plan is predicated on the validity of the following five assumptions:

- Security-Related Information

1.3 Plan Development

The Business Continuity Management Team (BCMT), with assistance from key internal support organizations and personnel, is responsible for developing the Plan. Development and support of individual product/platform disaster recovery plans are

the responsibility of the respective functional area. See Table 5.1-1, Team Organization.

1.4 Plan Maintenance

The BCMT is responsible for updating the Plan; testing the updated Plan; and training personnel.

Security-Related Information

Security-Related Information, the BCMT initiates a complete review of the Plan. Revisions are distributed to all authorized personnel.

1.5 Plan Testing

The Plan is Security-Related Information. The results are documented and evaluated for Plan updates.

2 Assessing Business Risk and Impact of Potential Emergencies

A key part of the BCP process is the assessment of potential risks to the business that could result from disasters or emergency situations. The purpose of hazard identification and risk assessment is to determine:

- (1) the events and environmental surroundings that can adversely affect NeuStar facilities by disruption as well as disaster
- (2) the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss.

2.1 Emergency Incident Assessment

The hazards and threats facing NeuStar and its data centers are those common to telecommunications companies of its size and location. These include, but are not limited to, the following:

- Security-Related Information

- Security-Related Information

The hazard identification and risk assessment determines what can occur, when and how often it is likely to occur, and how significant the effects could be. The hazard identification includes the types of hazards presented in the following subsections.

2.1.1 Environmental Disasters

The following are the natural events that have been considered as part of hazard identification.

Table 2.1-1. Environmental Disasters

Incident	Description	Assessment
Tornado	Tornadoes are tight columns of circling air creating a funnel shape. The wind forces within the tornado can reach over 200 miles per hour. Tornadoes can often travel in excess of 50 miles per hour. They can cause significant structural damage and can also cause severe injuries and death.	Possible but not frequent. Immediate power supply to ^{Security-Related} sites is underground.
Hurricane	Hurricanes are storms with heavy circular winds exceeding 60 miles per hour. The eye or center of the hurricane is usually calm. The hurricane contains both extremely strong winds and torrential rain. Hurricanes can cause flooding, massive structural damage to homes and business premises with associated power failures, and even injury and death.	Security-Related Information are subject to hurricane-induced weather but are perceived as being far enough inland to avoid the worst affects of these storms.

Incident	Description	Assessment
Flood	Floods result from thunderstorms, tropical storms, snow thaws or heavy and prolonged rainfall causing rivers to overflow their banks and flood the surrounding areas. Floods can seriously affect buildings and equipment causing power failures and loss of facilities and can even result in injury or death.	<p>Drainage/ flooding is not a problem in Security-Related Information.</p> <p>Air conditioning in Security-Related Information is internal to each data center. Water detection sensors are present at both sites.</p>
Snowstorm	Snowstorm conditions can include blizzards, strong winds and freezing temperatures with significant amounts of snow. Snow and ice can impact power and communications and employees may be unable to travel to work due to the impact on public transport or road conditions. It is possible for buildings to collapse under the weight of snow and injuries or even death could occur through freezing temperatures and icy conditions.	<p>Security-Related Information</p> <p>are subject to winter ice storms. Snow events are rare in Security-Related Information and relatively infrequent and moderate in Security-Related Information.</p>
Earthquake	Earthquakes are caused by a shifting of the earth's rock plates beneath its surface resulting in violent shaking and movement of the earth's upper surface. Severe earthquakes can destroy power and communication lines and disrupt gas, water and sewerage services. Significant damage to structures can occur including total collapse of buildings, bridges or other elevated structures. Earthquakes can also bring landslides, damage to dams, and aftershocks and resulting damage can hinder rescue efforts. In addition to being trapped in a collapsing building, of particular danger to human life is the possibility of falling glass or other objects.	<p>Security-Related Information</p> <p>is in an earthquake zone.</p>
Lightning Storms	The impact of lightning strikes can be significant. It can cause disruption to power and can also cause fires. It may also damage electrical equipment including computer systems. Structural damage is also possible through falling trees or other objects.	<p>Security-Related Information</p> <p>are equipped with both UPS and a backup generator, and both are grounded and surge protected.</p>

Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.

Incident	Description	Assessment
Fire	<p>Fires are often devastating and can be started through a wide range of events that may be accidental or environmental. Deliberate fires caused through arson are dealt with in the next section. The impact on the business will vary depending on the severity of the fire and the speed within which it can be brought under control. A fire can cause human injury or death and damage can also be caused to records and equipment and the fabric or structure of premises.</p>	<p>Security-Related Information is in an environmental fire hazard area.</p>
Subsidence and Landslides	<p>Subsidence and landslides are often caused through a change in the composition of the earth's surface. This change can often result from flooding, where flowing water can create cavernous open areas beneath structures. Subsidence or landslides can cause structural damage and can also disrupt transport services and affect traveling conditions.</p>	<p>Security-Related Information is in subsidence and landslides hazard environments.</p>

Security-Related Information

Security-Related Information

Security-Related Information

2.1.6 Pandemic

Table 2.1-6. Pandemic

Incident	Description	Assessment
Pandemic Event	Pandemic events, while they cannot be predicted, have the potential to affect the health of the human population. Particular to a corporation, pandemic	NeuStar will work with local health officials to contain pandemic events. If quarantined, critical personnel

Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.

Incident	Description	Assessment
	events can cause prolonged work absences.	are equipped to work remotely.

2.1.7 Loss of Key Personnel

Table 2.1-7. Loss of Key Personnel

Incident	Description	Assessment
Loss of Key Personnel	Loss of key personnel can negatively impact the ability to effectively respond and recover from an incident in a timely manner.	NeuStar identifies alternates for key personnel, as well as an order of succession for key positions in the event that primary staff members are unavailable.

2.2 Business Risk Assessment

The Business Risk Assessment helps the BCMT assess the criticality of NeuStar’s business processes and allows the team to determine operational and financial impact due to loss of services or reduction in service levels.

2.3 Business Impact Analysis (BIA)

The BIA enables the Business Continuity and Disaster Recovery Teams to:

- Identify critical systems, processes, functions, and their interdependencies.
- Assess the economic impact of incidents and disasters.
- Develop recovery time objectives.

2.4 Critical Business Functions and Recovery Time Objectives (RTO)

The Recovery Time Objective is a measure of the period between a disaster occurring and when the business determines the function must be available. NeuStar’s management and staff will need to complete the following tasks during the recovery time periods:

- Respond to the initial event.
- Complete an assessment of the circumstances of the interruption.
- Make an alert/declaration decision if required.
- Notify all staff, key vendors, and key customers.
- Relocate staff to alternate site(s).

- Establish the necessary resources at the alternate site(s).
- Resume critical business functions at an emergency level of service.

Table 2.4-1. Critical Business Functions and Recovery Time Objectives (RTO)

Product / Infrastructure	Department	Function	RTO
Corporate Infrastructure	Finance	General Ledger: accounts payable, fixed assets	Security-Related Informa
		Accounts Receivable	Security-Related Infor
		Payroll	Security-Related Informa
		Stock Options	Security-Related Infor
		<i>Billing:</i>	
		LNP Billing	Security-Related Infor
		Registry Billing	Security-Related Infor
		PAS Billing	Security-Related Infor
		CARE Billing	Security-Related Infor
		Identibase Billing	Security-Related Infor
	NANPA Billing	Security-Related Infor	
	NTS Billing	Security-Related Infor	
	Legal	In House Counsel Contracts Service Agreements Security Policy	Security-Related Informa
	Human Resources	Organization Development Reward and Recognition Benefits Employee Assistance Plan EAP, staff communications	Security-Related Ir
External Affairs	External Communications with regulatory/policy-making organizations and agencies	Security-Related Ir	
Corporate Communications	External Communications with the public including media, industry analysts, and investors.	Security-Related Ir	
Procurement	Purchasing	Security-Related Infor	
Facilities Management	Mailroom Office Services	Security-Related Ir	
Security-Related Information			Security-Related Ir
Security-Related Information			Security-Related Ir

Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.

Product / Infrastructure	Department	Function	BTO
<h1>Security-Related Information</h1>			
Enterprise Services	Registry Operations	Customer Service Operational Support	Security-Related Info
Carrier Services	NPAC Operations	NPAC SMS apps support	Security-Related Information
	NPAC Customer Service	Help Desk	Security-Related Ir
		Customer Outreach	Security-Related Informa
	PAS	Pooling Administration Code Administration	Security-Related
	OMS LSR (local service request)	LSR operations/apps support, customer service	Security-Related Informa
CARE	CARE operations/apps support, customer service (handled jointly with LSR)	Security-Related Informa	

Printed copies of this document are uncontrolled and are subject to change without notice. The master copy of this document can be found in Document Management.

3 Recovery and Restoration Planning

3.1 Recovery Phase

From a business perspective, a critical part of the BCP is the Recovery Phase. This phase deals with activating and failing over to the secondary data center in the shortest possible time to get applications and critical processes back up and running. Recovery steps and secondary site procedures are maintained internally and are specific to each line of business.

3.2 Restoration Phase

The time required for recovery of the primary data center and the eventual restoration of normal processing depends on the damage caused by the disaster. The restoration process begins immediately after the disaster and takes place in parallel with recovery operations at the backup site.

The primary goal is to restore normal operations as soon as possible. Restoration steps are stored internally and are specific to each line of business.

4 NeuStar Communications Options

4.1 Telephone (Landline)

- Security-Related Information

4.2 Telephone (Mobile) or SMS

- Security-Related Information

4.3 E-mail

- Security-Related Information

4.4 IM

- Security-Related Information

In the event that both Internet and Telecommunications connectivity have been severed, the NOC supervisor on duty will triage the event until appropriate communication can be established. The supervisor on-duty will assign the role of communication liaison to one member of the team, who will be responsible for contacting senior management by one of the methods above.

4.5 GETS, WPS and TSP

NeuStar is an essential infrastructure service provider for the telecommunications industry. In the event of a crisis, NeuStar will have access to extended and enhanced telecommunications services.

Membership for each of these services are reviewed and revised on the same schedule as the Plan, or as needed.

4.5.1 GETS – Government Emergency Telecommunication Service

The Government Emergency Telecommunications Service (GETS) is an emergency service designed for use when national security and emergency preparedness (NS/EP) personnel are unable to complete emergency calls through their regular telecommunications means. GETS uses a calling card to provide Federal, State, local government, and industry NS/EP users with a higher probability of call completion during periods of natural or man-made disasters or emergencies that cause congestion or network outages. GETS features are implemented as software enhancements to the telephone switches throughout the Public Switched Telephone Network (PSTN).

4.5.2 WPS – Wireless Priority Service

The goal of the Wireless Priority Service (WPS) is to provide an end-to-end nationwide wireless priority communications capability to key national security and emergency preparedness (NS/EP) personnel during natural or man-made disasters or emergencies that cause congestion or outages in the Public Switched Telephone Network (PSTN). Eligible users (see criteria at <http://wps.ncs.gov>) are key Federal, State, local, and tribal government and critical industry personnel who have NS/EP missions. WPS is complementary to, and can be most effective when used in conjunction with, the Government Emergency Telecommunications Service (GETS) to ensure a high probability of call completions in both the wireline and wireless portions of the PSTN. WPS serves NS/EP communications needs while minimizing impact on consumer access to the public wireless infrastructure.

4.5.3 TSP – Telecommunications Service Priority

The Telecommunications Service Priority (TSP) Program provides national security and emergency preparedness (NS/EP) users priority authorization of telecommunications services that are vital to coordinating and responding to crises. Telecommunications services are defined as the transmission, emission, or reception of intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio visual or other electronic, electric, electromagnetic, or acoustically coupled means, or any combination thereof. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors may become overwhelmed with requests for new telecommunications services and requirements to restore existing telecommunications services. The TSP Program provides service vendors with a Federal Communications Commission (FCC) mandate for prioritizing service requests by identifying those services critical to NS/EP. A telecommunications service with a TSP assignment is assured of receiving full attention by the service vendor before a non-TSP service.

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

- Security-Related Information

- Security-Related Information

Appendix A – NPAC Contractual Obligations

The following Contractor obligations and Customer rights apply in the event of a permanent loss of Contractor's NPAC/SMS Data Centers:

(a) Security-Related Information

(b) Security-Related Information