NeuStar Business Continuity Plan

neustar™

neustar	**Doc Title:**	*NeuStar Business Continuity Plan*	operational excellence Aspire Even Higher
	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

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

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 Informa, 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-Relate 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.	Drainage/ flooding is not a problem in Security-Related Information. Air conditioning in Security-Related Information is internal to each data center. Water detection sensors are present at both sites.
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.	Security-Related Information are subject to winter ice storms. Snow events are rare in Security-Related Informat and relatively infrequent and moderate in Security-Related Infor.
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.	Security-Related Information is in an earthquake zone.
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.	Security-Related Information are equipped with both UPS and a backup generator, and both are grounded and surge protected.

Incident	Description	Assessment
Fire	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.	Security-Related Information is in an environmental fire hazard area.
Subsidence and Landslides	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.	Security-Related Information is in subsidence and landslides hazard environments.

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

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

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 (RT0)

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 Infon
		Billing:	
		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 Ir

Product / Infrastructure	Department	Function	RTO
Security-Related Information			
Enterprise Services	Registry Operations	Customer Service Operational Support	Security-Related Infor
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-Relatec
	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

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

NEUSTAR CODE OF CONDUCT

1. Neustar will never, directly or indirectly, show any preference or provide any special consideration to any company that is a telecommunications service provider, which term as used herein shall have the meaning set forth in the Telecommunications Act of 1996.

2. No shareholder of Neustar shall have access to user data or proprietary information of the telecommunications service providers served by Neustar (other than access of employee-shareholders of Neustar that is incident to the performance of NANPA and LNPA duties).

3. Shareholders of Neustar will ensure that no user data or proprietary information from any telecommunications service provider is disclosed to Neustar (other than the sharing of data incident to the performance of NANPA and LNPA duties).

4. Confidential information about Neustar's business services and operations will not be shared with employees of any telecommunications service provider. Neustar shareholders will guard their knowledge and information about Neustar's operations as they would their own proprietary information.

5. No person employed by, or serving in the management of any shareholder of Neustar will be directly involved in the day-to-day operations of Neustar. No employees of any company that is a telecommunications service provider will be simultaneously employed (full-time or part-time) by Neustar.

6. Warburg Pincus will not control more than 40% of Neustar's Board.

7. No member of Neustar's board will simultaneously serve on the board of a telecommunications services provider.

8. No employee of Neustar will hold any interest, financial or otherwise, in any company that would violate the neutrality requirements of the FCC or the NPAC Contractor Services Agreements (the Master Agreements).

9. Neustar will hire an independent party to conduct a neutrality review of Neustar, ensuring that Neustar and its shareholders comply with all the provisions of this Code of Conduct. The neutrality analyst will be mutually agreed upon by Neustar, the FCC, NANC and the LLCs. The neutrality review will be conducted quarterly. Neustar will pay the expenses of conducting the review. Neustar will provide the analyst with reasonable access to information and records necessary to complete the review. The results of the review will be provided to the LLCs, to the North American Numbering Council and to the FCC and shall be deemed to be confidential and proprietary information of Neustar and its shareholders.

neustar™

CORPORATE CODE OF BUSINESS CONDUCT
NEUSTAR, INC.

Summary

The Code of Business Conduct has been adopted by the Board of Directors of Neustar, Inc. to provide standards by which directors, officers, employees and individual contractors providing services to or on behalf of the Company will conduct themselves in order to protect and promote organization-wide integrity and to enhance the Company's ability to achieve its mission.

The Code is designed to give you useful guidance about the way employees are to do business every day. As a representative of Neustar, it is your responsibility to read and understand this Code and to comply with it both in letter and spirit. The Code of Business Conduct applies to all directors, officers, employees and individual contractors providing services to or on behalf of the Company, who, unless otherwise specified, are referred to as "employees." The term "the Company" or "Neustar" means Neustar, Inc. and each of its divisions, subsidiaries and operating or business units unless otherwise specified.

The Code of Business Conduct is in addition to our obligations under the Neustar Code of Conduct, which has been adopted to ensure that Neustar maintains its obligation of neutrality in its business activities, and under other policies set forth in the Neustar employee handbook.

What you will see in the pages that follow are a series of conduct and ethical guidelines. Most of what you will read probably won't surprise you, for the overarching theme of these guidelines can be summed up this way: *As a representative of the Company, you must act with honesty and integrity in all matters.*

The Company expects each employee to conduct the business and affairs of the Company in a manner consistent with the Code of Business Conduct.

General Principles of the Code

Compliance with Laws. Employees must follow the law wherever they are around the world.

Honesty and Integrity. Employees must accurately and honestly represent the Company and will not engage in any activity or scheme intended to defraud anyone. Employees will act with candor and honesty in their communications with our stockholders and potential investors, and our attorneys and auditors.

Conflicts of Interest. Employees should avoid actual and perceived conflicts of interest. All employees owe a duty of undivided and unqualified loyalty to Neustar and should avoid any activity that is or has the appearance of being hostile or adverse to, or competitive with, Neustar or that interferes with the proper performance of their duties, responsibilities or loyalty to Neustar.

Financial and Business Records. Financial and business records - both for internal activities and external transactions - must be timely and accurate.

Use of Company Assets. Company assets – which include but are not limited to computers, software, materials and work time – must not be used for personal benefit (except for incidental and immaterial personal use of Company assets in accordance with this Code).

Working with Customers and Suppliers. Customers and suppliers must be dealt with fairly and with candor and honesty. Avoid excessive or lavish gifts that may give the appearance of undue influence and personal financial transactions with customers and suppliers that may influence your ability to perform your job.

Working with Governments. The public trust associated with transactions between the private sector and government entities imposes special responsibilities on Company employees and representatives to adhere to the same high standard of conduct expected of the government employee. Company

employees shall take no actions that would cause the government employee to violate, to appear to violate, or that would be otherwise inconsistent with, that standard of conduct.

Protecting Information. Every Company employee has an obligation actively to protect and safeguard the Company's confidential, sensitive and proprietary information, in a manner designed to prevent the unauthorized disclosure of such information.

Information about Other Companies. Employees must respect the nonpublic information of other companies, including our competitors. Although collecting information on our competitors from legitimate sources to evaluate the relative merit of their products, services and marketing methods is proper and often necessary, any form of questionable intelligence gathering is strictly against the Code.

Violations of the Code include asking other employees to violate the Code, not reporting a Code violation or failing to cooperate in a Code investigation. Any retaliation against an individual who reports a violation of this Code or of law in good faith, or who assists in the investigation of a reported violation, is itself a serious violation of the Code and applicable law.

You are expected to adhere to the Code. Violating the Code may result in disciplinary action, up to and including termination of your relationship with Neustar.

Your Responsibilities

- These principles are not the entire Code of Business Conduct – they are the principles underlying the Code. It is your responsibility to read and understand the Code of Business Conduct which follows and is available for viewing on the Neustar Home Page at www.Neustar.biz.
- You must comply with the Code in both letter and spirit. Ignorance of the Code will not excuse you from its requirements.
- Follow the law wherever you are and in all circumstances.
- Never engage in behavior that harms the reputation of the Company. If you wouldn't want to tell your parents or your children about your action - or wouldn't want to read about it in a newspaper – don't do it.
- Some situations may seem ambiguous. Exercise caution when you hear yourself or someone else say, "Everybody does it," "Maybe just this once," "No one will ever know" or "It won't matter in the end." These are signs to stop, think through the situation and seek guidance. Most importantly, don't ignore your instincts. Ultimately, you are responsible for your actions.
- You have several options for seeking guidance. You may discuss concerns with your manager, other members of management, or the responsible employees in the Human Resources or Legal Department. Directors and executive officers should contact the Legal Department or the Chair of the Audit Committee.

Employees are obligated to report violations, and suspected violations, of the Code. This includes situations where a manager or colleague asks you to violate the Code. In all cases, there will be no reprisals for making a report in good faith, and every effort will be made to maintain confidentiality.

- The reporting of a violation of the Code in bad faith, a frivolous report of a violation of the Code, or a fabricated report of a violation of the Code will be considered a violation of the Code.

You can report violations and suspected violations of the Code:

- to your manager or higher levels of management, the Senior Vice President of Human Resources, or the Company's General Counsel; or
- through the Company's Compliance Hotline or Web Form.

If you wish to make a report anonymously, you may do so by using the Compliance Hotline or Web Form.

If an accounting or auditing matter is involved, concerns or reports of violations may also be submitted by email to the Audit Committee.

Members of the Board should report potential violations to the General Counsel or the Audit Committee chair.

Contact information for reporting potential violations through the mechanisms described above can be found on the page at the end of the Code titled "Contact Information for Reporting Violations."

- Employees are obliged to cooperate with investigations under the Code. Employees must understand the Code, seek guidance when necessary and report suspected Code violations. If a manager knows that an employee is contemplating a prohibited action and does nothing, the manager may be held responsible along with the employee.
- If you have questions about any situation or if there is any uncertainty about how an action may be interpreted, ask. Always ask.

This Code should help guide your conduct. But the Code cannot address every circumstance and isn't meant to; this is not a catalogue of workplace rules. You should be aware that the Company has policies in such areas as securities trading and workplace conduct. Employees should consult the policies of Neustar in specific areas as they apply.

- The most important message is this: When you are uncertain about any situation, ask for guidance.

The Code of Business Conduct is not an express or implied contract of employment and does not create any contractual rights of any kind between Neustar and its employees. The Code does not modify the employment relationship between an employee and the Company, whether at-will or governed by contract. In addition to the Code, there are other standards governing the conduct of Neustar employees with which each Neustar employee is required to comply.

Neustar reserves the right to amend, alter or terminate the Code at any time for any reason.

Compliance with Laws

Employees must follow the law wherever they are around the world.

A fundamental principle of Neustar is that its employees will comply with all applicable law wherever they are around the world.

Honesty and Integrity

Employees must accurately and honestly represent the Company and will not engage in any activity or scheme intended to defraud anyone. Employees will act with candor and honesty in their communications with our stockholders and potential investors, and our attorneys and auditors.

Conflicts of Interest

All employees owe a duty of undivided and unqualified loyalty to Neustar. Employees should avoid actual and perceived conflicts of interest and should avoid any activity that is or has the appearance of being hostile or adverse to, or competitive with, Neustar or that interferes with the proper performance of their duties, responsibilities or loyalty to Neustar.

Overview

Your personal activities and relationships must not conflict, or appear to conflict, with the interests of the Company. Keep in mind, the Code can't specifically address every potential conflict, so use your conscience and common sense. When confronted with any situation that may be perceived as a conflict of interest, even if you don't believe the situation would violate this Code, or when unsure about proper conduct, you should seek guidance from your principal manager, any member of management or responsible employees in the Human Resources or the Legal Department. When questions arise, seek guidance.

General Principles

- Avoid situations where your personal interests conflict, or appear to conflict, with those of the Company.
- Any actual or potential conflict of interest must be reported to the General Counsel. Employees who are unsure whether they are involved in a conflict of interest or whether an action might create a conflict of interest should seek guidance, as discussed above. A conflict of interest or potential conflict of interest may be resolved or avoided if it is appropriately disclosed and approved in accordance with the procedures below. In some instances, disclosure may not be sufficient and the Company may require that steps be taken to avoid a conflict of interest or that conduct be stopped.
- You may own up to 1% of the stock in a competitor, customer or supplier without seeking prior approval from the General Counsel and Chief Financial Officer so long as the stock is in a public company and you do not have discretionary authority in dealing with that company. If you want to purchase more than 1% of the stock in a customer, competitor or supplier, or if the company is nonpublic or you have discretionary authority in dealing with that company, then the stock may be purchased only with prior approval of the General Counsel and the Chief Financial Officer.
- If you have a financial or other interest in a transaction between the Company and a third party – even an indirect interest through, for example, a family member, close relative or a close friend, or if there is any other potential or actual conflict of interest – and you are in a position to influence that transaction, that interest must be disclosed to the General Counsel prior to the transaction when you become aware of it.

  You may not take for yourself or disclose to others outside the Company any opportunity for financial gain that you find out about because of your position at Neustar or through the use of Company property or information.

  You may not participate in a "Friends or Family" security offering of other companies if the offer was made to you because of your position at Neustar.
- You may not directly or indirectly conduct outside business that interferes with the proper performance of your job at Neustar, is conducted during normal working hours, utilizes Neustar confidential information or puts you in a situation where Neustar confidential information may be used intentionally or unintentionally.
- Any potential conflict of interest must be approved in advance by the General Counsel. Any potential conflict of interest that involves an officer of the Company or of a subsidiary must be approved in advance by the General Counsel and Chief Operating Officer (or if there is no Chief Operating Officer, the Chief Executive Officer). Any potential conflict of interest that involves a director or an

executive officer of the Company must be approved by the Board of Directors or its designated committee.

- Loans from the Company to directors and executive officers are prohibited. Loans from the Company to other officers and employees must be approved in advance by the Board of Directors or its designated committee.

Financial Records

Financial and business records - both for internal activities and external transactions - must be prepared in a timely manner and must be accurate.

Overview

Every company financial and business record--including time sheets, sales records and expense reports-must be accurate, prepared in a timely manner and in accordance with the law. These records are the basis for managing the Company's business and for fulfilling its obligations to stockholders, employees, customers, suppliers and regulatory authorities. Employees should not enter into side letters to contracts or similar arrangements without prior approval of the Chief Financial Officer and/or General Counsel. It is the responsibility of each employee to make sure that every business record which he or she deals with is accurate, complete and reliable.

If you know of violations by others, take note: You must report those instances, or you are in violation of the Code. Accurate records are everyone's responsibility. It's always a good idea to double-check them.

General Principles

- Always record and classify transactions in the proper accounting period and in the appropriate account and department. Delaying or prepaying invoices to meet budget goals is a violation of the Code.
- All financial reports, accounting records, contracts, research reports, expense accounts, time sheets and other documents must accurately and clearly represent the relevant facts or the true nature of the transaction. Employees should not enter into side letters or other arrangements to contracts without prior approval of the Chief Financial Officer and/or General Counsel.
- Never falsify any document or distort the true nature of any transaction. All transactions must be supported by accurate documentation.
- All reports made to regulatory authorities, and other public communications, should contain disclosure that is full, fair, accurate, complete, timely and understandable.
- Employees must cooperate with investigations into the accuracy and timeliness of financial records. To the extent estimates and accruals are necessary in company reports and records, they must be supported by appropriate documentation and based on good faith judgment.
- Payments may only be made to the person or the firm that actually provided the goods or services.

Use of Company Assets

Company assets – which include but are not limited to computers, software, materials and work time – must not be used for personal benefit.

Overview

Company assets are meant for Company, not personal, use. Company assets include your time at work and work product, as well as the Company's equipment and vehicles, computers and software, Company information, and trademarks and name.

Common sense should prevail, of course. Incidental and immaterial personal use of Company assets such as computers and other equipment, telephones, and supplies, is permitted. Frequent or excessive use of such items, however, represents misuse. Theft or deliberate misuse of Company assets is a violation of the Code.

General Principles

- You may not use the Company's assets for your personal benefit or the benefit of anyone other than the Company.
- Company computer systems and equipment are meant for Company use only. For example, they should never be used for outside businesses, illegal activities, gambling or pornography.
- Company information is an asset of the Company and must be used and protected appropriately.
- Misuse of Company assets may be considered theft and result in termination or criminal prosecution. You must have permission from your principal manager before you use any Company asset -- including information, work product or trademark--outside of your Company responsibilities.
- Before accepting payment for speeches or presentations related to the Company or your work at the Company, always get your principal manager's approval.

Working with Customers and Suppliers

Customers and suppliers must be dealt with fairly with candor and honesty. Avoid excessive or lavish gifts that may give the appearance of undue influence and personal financial transactions with customers and suppliers that may or may appear to influence your ability to perform your job.

Overview

It often is customary to exchange gifts and entertainment with customers and suppliers. The key is to keep an arm's length relationship. Also, you should know that special restrictions apply when dealing with government employees. For more information, see the next section on Working with Governments. In all cases, when in doubt, seek guidance.

General Principles

- The Code prohibits employees from accepting lavish or excessive gifts or entertainment. This is an area in which your judgment is critical. For instance, modest holiday gifts are usually fine. But an expensive weekend trip probably would not be. If you are uncertain, seek guidance from your principal manager.

  In some limited circumstances it may be customary or appropriate to entertain customers and accept entertainment from suppliers. It similarly may be customary and appropriate to arrange or take part in programs and events that include meals and lodging. For example: Business meal discussions with a customer or supplier are legitimate. Speaking at a continuing education program where the sponsor pays for the related travel and lodging is acceptable. It generally is not appropriate for an employee to accept a supplier’s invitation to attend an entertainment or sporting event at the supplier’s expense, although it may be appropriate if it demonstrably helps to build or maintain a business relationship. You must obtain permission from your principal manager before accepting such an invitation.

- Gifts and entertainment for customers, potential customers and suppliers must support the legitimate business interests of the Company and should be reasonable and appropriate under the circumstances. Always be sensitive to our customers' and suppliers' own rules on receiving gifts and entertainment.

- Company stock cannot be given as a gift on behalf of the Company under any circumstances.

- Consistent with the obligation we all have to act with integrity and honesty at all times, you should deal fairly with the Company's customers, suppliers, competitors and employees. No officer or employee should take unfair advantage of anyone through misrepresentation or any unfair business practice.

  Under no circumstances should you offer or accept any bribes or kickbacks. If any bribe or kickback is offered to you, you should immediately report the incident to the General Counsel.

Working with Governments and Internationally

The public trust associated with transactions between the private sector and foreign or U.S. government entities imposes special responsibilities on Company employees and representatives to adhere to the same high standard of conduct expected of the government employee. Company employees shall take no actions that would otherwise cause the government employee to violate, to appear to violate, or that would be otherwise inconsistent with, that standard of conduct. Also, in transacting with foreign governments, persons, and organizations, the Company is mindful of the additional restrictions and responsibilities imposed by U.S. laws and regulations. Company employees must take all necessary precautions to comply with all applicable provisions.

Overview

Conducting business with governments is not the same as conducting business with private U.S. parties. These transactions often are covered by special legal rules. No Company employee may offer or give anything of monetary value, including gifts, gratuities, favors, entertainment or loans, to an employee of a U.S. or foreign government agency, unless prior approval from the Legal and External Affairs Department has been obtained. In addition, neither the Company nor an individual acting on behalf of the Company may make political contributions, even where they are permitted by law. If you make a political contribution, it must be clear that you are acting as an individual and not as a representative of the Company. The Company will not reimburse you for any personal political contributions you make. You should consult with the Legal and External Affairs Department to be certain that you are aware of applicable rules. You must have the written approval of the Legal and External Affairs Department before providing anything that might be considered to be excessive value or non-routine to a government official or a candidate for public office. Under no circumstances can anything be given to a government official or candidate for office that (i) is intended to improperly influence any act or decision of such official, employee, or candidate for the purpose of promoting the business interests of Neustar in any respect, or (ii) would violate the governmental official's or political candidate's own professional ethical standards. Should you have any questions whatsoever about what is appropriate and what is not, you must consult with the Legal and External Affairs Department.

The Company prohibits the payment of bribes to U.S. and foreign government officials. Payments to foreign government officials are governed by the Foreign Corrupt Practices Act ("FCPA"). "Government officials" are employees of any government anywhere in the world, even low-ranking employees or employees of government-controlled entities. The term "government officials" also includes political parties and candidates for public office. It is your obligation to understand whether someone you deal with is a government official. If there are any questions concerning someone's status as a government official, consult the Legal and External Affairs Department.

In some countries it may be customary at times to pay government employees for performing their required duties. These, too, are governed by the FCPA. Facilitating payments, as they are known, are small sums paid to facilitate or expedite routine, non-discretionary government actions and may or may not be appropriate under the FCPA or laws of the foreign country. In contrast, a bribe, which is never permissible, is giving, promising or offering to give anything of value to a government official, his or her relatives, associates or other affiliated persons or organizations with the intention of influencing a discretionary decision of the government official. The prohibition extends not only to employees, officers and directors of the Company, but also to agents, subcontractors and other intermediaries, and should be reflected in any agreements with customers, vendors and agents.

Understanding the difference between a bribe and a facilitating payment is critically important. All facilitating payments must be approved in advance by the Chief Executive Officer, Chief Financial Officer and General Counsel, and recorded appropriately.

Further, the Company is committed to complying with all laws and regulations governing transactions involving non-U.S. governments, persons and organizations. The laws and regulations applicable to such dealings include, but are not limited to, the FCPA as noted above, the regulations administered by the Office of Foreign Asset Control ("OFAC") and the Bureau of Industry and Security ("BIS"), and U.S. antiboycott provisions. The United States has restrictions in place with respect to conducting business with certain countries, their governments and nationals, and certain individuals and organizations associated with embargoed countries or subject to trade restrictions for other reasons, as identified on lists maintained by the U.S. government. No one acting on behalf of the Company may be involved in business arrangements or otherwise engage in transactions with or involving sanctioned countries, nationals or entities in violation of U.S. laws and regulations. In addition, no one acting on behalf of the Company may engage, directly or indirectly, in transactions with “Specially Designated Nationals and Blocked Persons,” or with those identified on the "Denied Persons List," the Entity List," or "Unverified List" in violation of U.S. laws and regulations. If you have questions about these or other restrictions, you must contact the Legal and External Affairs Department.

Our Company and its subsidiaries must comply with all applicable trade restrictions and boycotts imposed by the U.S. government. (A boycott is a restriction on a company's ability to ship goods into a specific country or do business there.) Moreover, our Company and its subsidiaries also must abide by U.S. anti-boycott laws that prohibit companies from participating in any international boycott not sanctioned by the U.S. government, and that impose certain reporting requirements concerning requests to comply with, further or support unsanctioned boycotts. This includes, for example, a request to provide information concerning our Company's dealings with boycotted countries. Any such requests and any questions generally concerning boycotts and antiboycott obligations should be reported to the Legal Department.

General Principles

- The ban on bribes applies to all governments, foreign and domestic, and extends to third parties acting on behalf of the Company, including all contractors and consultants. Employees must not engage a vendor, contractor or consultant if the employee has reason to believe that the contractor or consultant may attempt to bribe a government official.
- Employees must comply with all U.S. trade laws and regulations including, but not limited to, the FCPA, OFAC and BIS regulations, and U.S. antiboycott requirements. Any questions or concerns regarding the permissibility of a certain transaction or other dealing are to be brought to the Legal Department.
- The Company may hire government officials or employees to perform services that have a legitimate business purpose, but only pursuant to a written agreement and with the prior approval of the Legal and External Affairs Department. Government officials should never be hired to perform services that conflict with their official duties.
- All facilitating payments must be documented in written agreements with the receiving government official, and approved in advance by the Chief Executive Officer, Chief Financial Officer and General Counsel, and recorded as required by applicable laws and regulations.
- The Company does not make any political contributions, even where they are permitted by law. If you make a political contribution, it must be clear that you are acting as an individual and not as a representative of the Company.
- Employees will not be reimbursed for political contributions. Your job will not be affected by your choices in personal political contributions.
- Employees must comply with all U.S. boycott and anti-boycott requirements.

Protecting Information

Every Company employee has an obligation actively to protect and safeguard the Company's confidential, sensitive and proprietary information in a manner designed to prevent the unauthorized disclosure of such information.

Overview

It is your obligation to safeguard the Company's nonpublic information. Some Neustar information may not be appropriate for sharing within the Company. Before disclosing nonpublic information to others within the Company, be sure that it is appropriate for them to have access to the information. In addition, you should not share the Company's nonpublic information with anyone outside the Company unless it is necessary as part of your work responsibilities and appropriate safeguards are in place. This obligation is in addition to any confidentiality or nondisclosure agreements you may have executed.

Nonpublic information is any information that has not been disclosed or made available to the general public. Trading in stocks or securities based on nonpublic information, or providing nonpublic information to others so that they may trade or make further disclosures, is illegal and may result in prosecution.

Nonpublic information includes items such as financial or technical data, financial plans and projections, customer lists, plans for acquisitions or divestitures, new products, software code, software development plans, inventions or marketing campaigns, personal information about employees, major contracts, expansion plans, financing transactions, major management changes and other corporate developments. If in doubt, consider the information nonpublic.

In any circumstances in which any Neustar representative is considering disclosing potentially material, nonpublic information, the representative must check with Neustar's Legal Department before such information is disclosed to determine whether the information has already been publicly disclosed and whether the information is material. In any circumstances in which potentially material information has been improperly disclosed, the General Counsel must be notified immediately.

There are specific policies in place for disclosure of information with the media and financial communities. No employee should speak with anyone in the media or financial community without complying with these policies.

General Principles

- Do not disclose nonpublic information to anyone outside the Company, except when disclosure is required for business purposes and appropriate steps have been taken to prevent misuse of the information.
- Employees may not buy or sell stocks or securities of Neustar or of other entities based on nonpublic information obtained from their work at the Company. There are specific policies that address securities trading in more detail and you must comply with these policies.
- Disclosing nonpublic information to others, including family and friends, is a violation of the Code and may violate the law.
- Consult with the General Counsel regarding retention of records in the case of actual or threatened litigation or governmental investigation.

Information about Other Companies

Employees must respect the nonpublic information of other companies, including our competitors. Although collecting information on our competitors from legitimate sources to evaluate the relative merit of their products, services and marketing methods is proper and often necessary, any form of questionable intelligence gathering is strictly against the Code.

Overview

The Company may receive information about other companies in a number of ways. Information obtained under a confidentiality agreement must be protected in the same manner as the Company protects its own confidential information and may only be used in accordance with the terms of the confidentiality agreement. Information that is publicly available or that is obtained from legitimate sources may be used to evaluate the relative merit of competitor's products, services and marketing methods.

Some methods of acquiring information are not proper. For example, Company employees should not seek confidential information from a new employee who recently left a competitor if doing so would induce that employee to violate any contractual obligations he or she may have to a former employer. Company employees should not misrepresent their identity in the hopes of getting confidential information about a competitor. Any form of questionable intelligence gathering is strictly against the Code.

Any trading of securities based upon nonpublic information in the Company's possession, whether it relates to the Company, its customers, suppliers, competitors or other third parties, is prohibited by this Code and is illegal. There are specific policies that address securities trading in more detail and you must comply with these policies.

Administration of the Code

All Company employees, directors, officers and contractors will receive or have access to a copy of this Code at the time they join the Company.

The Company expects each employee, director, officer and contractor to conduct the business and affairs of the Company in a manner consistent with the Code of Business Conduct. Failure to abide by the Code of Business Conduct or the guidelines for behavior that the Code of Business Conduct represents may lead to disciplinary action. For alleged violations of the Code of Business Conduct, the Company will weigh relevant facts and circumstances. Discipline will vary depending on the circumstances and may include, alone or in combination, a letter of reprimand, demotion, loss or reduction of bonus, suspension or even termination of service.

While the Company will generally attempt to communicate changes in the Code of Business Conduct concurrent with or prior to the implementation of such changes, the Company reserves the right to modify, amend or alter the Code of Business Conduct without notice to any person or employee. Failure to receive notification of any modification, amendment or alteration of the Code of Business Conduct will not excuse any failure to comply with the Code as so modified, amended or altered.

Any questions regarding interpretation of the Code should be directed to the General Counsel, Senior Vice President of Human Resources or the Chief Financial Officer. The provisions regarding administration of the Code may be varied as necessary in particular cases and as may be required to conform to local law or contract.

Approvals and Waivers

Any prior approvals required pursuant to the Code shall be obtained in writing from the appropriate person. A copy of the approval shall be provided to the General Counsel and the Senior Vice President of Human Resources and retained as required under the Company's document retention policies.

Any waiver of a provision of this Code for a director or an executive officer of the Company must be approved by the Board of Directors or its designated committee, recorded in writing, and disclosed to the extent required by law or regulation. Any waiver of a provision of this Code for individuals other than directors and executive officers must be approved in writing by the General Counsel and Chief Financial Officer. Copies of all waivers will be provided to the General Counsel. All waivers and approvals will be kept in the Legal Department and retained as required under the Company's document retention policies. Copies of all waivers and approvals will also be kept in the respective employee file, as appropriate.

Reporting and Investigation of Concerns Regarding Compliance with the Code

The Company expects that all employees will take all responsible steps to prevent a Code violation.

All employees are obligated to report violations and suspected violations of the Code of Business Conduct and any concerns they may have pertaining to non-compliance with the Code. You can report violations and suspected violations of the Code:

- to your manager or higher levels of management, the Senior Vice President of Human Resources, or the Company's General Counsel; or
- through the Company's Compliance Hotline or Web Form.

If you wish to make a report anonymously, you may do so by using the Compliance Hotline or Web Form. You should not use the Compliance Hotline or Web Form for personal grievances not involving this Code or violations of law. We would prefer that you identify yourself to facilitate our investigation of any report. However, you may choose to remain anonymous.

If an accounting or auditing matter is involved, concerns or reports of violations may also be submitted by email to the Audit Committee.

Members of the Board and executive officers should report potential violations to the General Counsel or the Audit Committee chair.

Contact information for reporting possible violations through the mechanisms described above can be found on the page at the end of the Code titled "Contact Information for Reporting Violations."

Any manager who receives a report of a potential violation of this Code must report it immediately to the General Counsel or Senior Vice President of Human Resources. Because failure to report wrongdoing can itself be understood to condone the wrongdoing, we emphasize the importance of reporting. Failure to report knowledge of wrongdoing may result in disciplinary action against those who fail to report.

We will hold complaints in confidence to the extent legally permissible. In accordance with applicable law, it is the policy of Neustar not to allow retaliation for reports of misconduct or reports of violations of this Code made in good faith. Retaliation in any form against an individual who reports a violation of this Code or of law in good faith, even if the report is mistaken, or who assists in the investigation of a reported violation, is itself a serious violation of this policy. Acts of retaliation should be reported immediately. Any employee who engages in retaliation is subject to discipline, up to and including termination, and in appropriate cases, civil and/or criminal liability.

All employee communications made in good faith will be treated promptly and professionally and without risk of retribution whatsoever. Any use of these reporting procedures in bad faith or in a false or frivolous manner will be considered a violation of this Code.

We will use reasonable efforts to protect the identity of the person about or against whom an allegation is brought, unless and until it is determined that a violation has occurred.

All reports will be taken seriously and investigated promptly. Ongoing investigations will not be discussed in a public forum. Any person involved in any investigation in any capacity of a possible misconduct must not discuss or disclose any information to anyone outside of the investigation unless required by law or when seeking his or her own legal advice, and is obligated to cooperate fully in any investigation.

Corrective and disciplinary action will be taken as necessary. Violations of the law will be reported through the Legal Department to the proper authorities.

Investigations

All reports of suspected Code violations will be forwarded to the General Counsel and Senior Vice President of Human Resources, except for complaints and concerns involving accounting or auditing matters, which will be handled in accordance with procedures established by the Audit Committee.

The responsibility for administering the Code and investigating violations of the Code rests with the Senior Vice President Human Resources and the General Counsel. If the alleged violation involves a director or executive officer, the Audit Committee shall have responsibility for investigation of the complaint. They will make a preliminary determination that will be communicated to the principal manager of the alleged violator. The General Counsel and Senior Vice President Human Resources, in conjunction with the Chief Financial Officer and other members of executive management, as appropriate, shall have sole authority for making the final determination whether a violation has occurred. If the alleged violation involves a director or executive officer, however, the Audit Committee shall have sole authority for making the final determination whether a violation has occurred. The subject of the investigation will be afforded an opportunity to respond to any allegations made against him or her if preliminary results of the investigation require a statement from the subject.

A person suspected of violating the Code may be suspended with or without pay while an investigation is conducted. The suspension will be at the discretion of the Senior Vice President of Human Resources and General Counsel, who may consider the recommendations of the employee's principal manager.

The Chief Financial Officer and the General Counsel will periodically report significant compliance issues to the Audit Committee of the Board of Directors, including significant reported Code violations, the status of such violations and, if applicable, the corrective actions taken.

Disciplinary Actions

Violations may result in disciplinary action. The Company will strive to impose discipline for each Code violation that fits the nature and particular facts of the violation. The Company generally will issue warnings or letters of reprimand for less significant, first-time offenses. Violations of a more serious nature may result in suspension without pay, demotion, loss or reduction of bonus, or any combination. Termination of service with the Company generally is reserved for conduct such as theft or other violations amounting to a breach of trust, or for cases where a person has engaged in multiple violations. Termination may also be appropriate for ethical violations if an individual has consciously chosen to pursue unethical behavior.

The authority to determine corrective and disciplinary action rests with the General Counsel and the Senior Vice President of Human Resources, in conjunction with the Chief Operating Officer (or if there is no Chief Operating Officer, the Chief Executive Officer) and other members of executive management, as appropriate, who may consider recommendations of the employee's principal manager.

The appropriate principal manager or a representative from Human Resources will communicate the final discipline decision.

A violator may seek reconsideration of the final discipline decision by submitting a written request for reconsideration within fourteen days of notification of the disciplinary action. The request for reconsideration will be considered by the General Counsel and Senior Vice President of Human Resources, in conjunction with the Chief Financial Officer and Chief Operating Officer (or if there is no Chief Operating Officer, the Chief Executive Officer), as may be suggested by the nature of the offense and mitigating circumstances.

A notation as to the final decision as well as any determinations of no violation, letters of reprimand or other written communications with the alleged violator will be placed in the employee's personnel file as part of his or her permanent record.

Violations of this Code are not the only basis for disciplinary action. The Company has additional policies, guidelines and procedures governing conduct, and violations of those policies, guidelines and procedures may also result in corrective or disciplinary action.

Signature and Acknowledgement

All new employees must sign an acknowledgment form confirming that they have read the Code and understand its provisions. Failure to read the Code or to sign an acknowledgment form, however, does not excuse an employee from the terms of this Code.

It's Up to You

Administration of the Code is everyone's responsibility. There are colleagues to help you do the right thing. If you act with integrity and seek guidance when you are uncertain, you'll be doing the right thing.

Questions and Answers about Procedures

The following questions and answers relate to procedures relevant to potential violations of the Code of Business Conduct.

It is our intent that these questions and answers be followed in most cases where a potential violation of the Code has occurred.

Reporting

Q. To whom should an employee report suspected violations of the Code?

A. You can report suspected violations of the Code: (a) to your manager or higher levels of management, the Senior Vice President of Human Resources, or the General Counsel; or (b) through the Company's Compliance Hotline or Web Form. If an accounting or auditing matter is involved, concerns or reports of violations may also be submitted by email to the Audit Committee. ***Contact information for reporting possible violations through these mechanisms can be found on the page at the end of the Code titled "Contact Information for Reporting Violations."***

Q. Will there be any retaliation for reporting in good faith a violation of the Code?

A. Absolutely not. Good faith reports of violations of the Code may be made without fear of reprisal or retaliation.

Q. Can an employee report a suspected violation of the Code confidentially?

A. Every effort will be made to maintain in confidence the identity of a person making a report of a suspected Code violation. Provision has been made for anonymous reporting of alleged violations.

Investigation

Q. Who should take the lead in investigating suspected Code violations?

A. The investigation normally will be conducted by the Senior Vice President of Human Resources and the General Counsel.

Q. Will the subject of the investigation receive notification of the investigation?

A. It depends on the circumstances and the results of the preliminary investigation. If there is insufficient evidence of a Code violation, the investigation may be closed without notification. In the event it is determined that evidence of a violation exists, the individual will be notified but that notification may not occur until after records have been reviewed and witnesses interviewed.

Q. Will the subject of the investigation have an opportunity to respond to any allegations made against him or her?

A. Maybe. The subject of an investigation will have the opportunity to respond to any allegations made against that person if the preliminary results of the investigation require a statement from the subject. The General Counsel or Senior Vice President Human Resources will determine whether such a statement is necessary.

Q. Can a suspected violator be suspended while an investigation is ongoing?

A. Yes, at the discretion of the Senior Vice President of Human Resources and General Counsel, a person suspected of violating the Code can be suspended with or without pay while an investigation is conducted.

Decision

Q. Who makes the decision on whether a violation of the Code has occurred?

A. A preliminary determination will be made by the Senior Vice President of Human Resources and the General Counsel (or by the Audit Committee if the investigation involves a director or executive officer). That preliminary determination will be communicated to the principal manager of the alleged violator. Sole authority for making a final determination that a violation has occurred rests jointly with the Senior Vice President of Human Resources and General Counsel, in consultation with the Chief Financial Officer and others as appropriate.

Discipline

Q. Does anyone make a recommendation on appropriate discipline?

A. Yes, the principal manager may make a recommendation on appropriate discipline. That recommendation should be given to the General Counsel and the Senior Vice President of Human Resources, who will determine the final disciplinary action, if any.

Q. What factors will be considered in determining the appropriate punishment?

A. The Company strives to impose discipline for a code violation that fits the nature and particular facts of a violation, including the history of those involved.

Q. What forms of discipline does the Company impose?

A. The Company generally will issue warnings or letters of reprimand for less significant, first-time offenses. Violations of a more serious nature may result in suspension without pay, demotion, loss or reduction of bonus or any combination. Termination of employment generally is reserved for theft or other violations amounting to a breach of trust, and for cases where a person has engaged in multiple violations. Termination may also be appropriate for ethical violations if the employee has consciously chosen to pursue unethical behavior.

Q. Can the violator seek reconsideration of the final discipline decision?

A. Yes, within 14 days of notification of the final discipline decision, the alleged violator can make a written request for reconsideration, which will be considered by the General Counsel and the Senior Vice President of Human Resources, in conjunction with the Chief Financial Officer and Chief Operating Officer (or if there is no Chief Operating Officer, the Chief Executive Officer).

Q. Who communicates the final discipline decision?

A. The appropriate principal manager or representatives from the Human Resources department.

Reporting and Record Keeping

Q. Do the Senior Vice President of Human Resources, Chief Financial Officer and General Counsel report the violation and discipline to anyone other than the violators?

A. Yes, the Senior Vice President of Human Resources, Chief Financial Officer, as appropriate, and General Counsel will report their final decision to the violator's principal manager and to the Audit Committee of the Board of Directors.

Q. What documents concerning the violation will be maintained in an employee's personnel records?

A. A notation as to the final decision as well as any letters of reprimand or other communications with the violator, including statements finding that there was no violation, will be placed in the employee's personnel file as part of his or her permanent record.

The Code of Business Conduct is not an express or implied contract of employment and does not create any contractual rights of any kind between Neustar and its employees. The Code does not modify the employment relationship between an employee and the Company, whether at-will or governed by contract. In addition to the Code, there are other standards governing the conduct of Neustar employees with which each Neustar employee is required to comply.

Neustar reserves the right to amend, alter or terminate the Code at any time for any reason.

Contact Information for Reporting Violations

Employees should report suspected Code violations: (a) to their manager or higher levels of management, the Senior Vice President of Human Resources, or the General Counsel; or (b) through the Company's Compliance Hotline or Web Form. If an accounting or auditing matter is involved, concerns or reports of violations may also be submitted by email to the Audit Committee.

Senior Vice President of Human Resources

Christine Brennan
21575 Ridgetop Circle
Sterling, VA 20166
Phone: (571) 434-5357

General Counsel

Scott Blake Harris
21575 Ridgetop Circle
Sterling, VA 20166
Phone: (202) 533-2920

Compliance Hotline and Web Form

The number for the Company's Compliance Hotline and the Web Form are located on the Company's Investor Relations website at www.Neustar.biz.

Accounting or Auditing Matters

Concerns or reports of potential violations related to accounting or auditing matters may by sent by email to the Audit Committee at CorporateCode@Neustar.biz.

Please find below:

- Survey Results for the past five years and
- Sample NPAC Performance Feedback Survey from 2012

For more detail on our Customer Satisfaction and Customer Service, Please See Proposal Section 2.5 which is attached to the IASTA tool in response to RFP Section 15.1 Option Attachments.

NPAC Survey Results for the Past Five Years

Year	Actual Score	Best Score	Industry Standard
2008	3.46	4.0	Exceptional
2009	3.66	4.0	Superior
2010	3.68	4.0	Superior
2011	3.80	4.0	Superior
2012	3.90	4.0	Superior

Score Key:

Equal or greater than 2.00 but less than 3.00 = Average
Equal or greater than 3.00 but less than 3.25 = Above Average
Equal or greater than 3.25 but less than 3.5 = Exceptional
Equal or greater than 3.5 but less than 4.0 = Superior

Welcome to the Number Portability Administration Center (NPAC) Users Survey. Neustar would like to obtain your feedback and comments concerning your interaction with the NPAC. Your response will be forwarded to Neustar's Business Operations group for evaluation and will assist us in better meeting your future needs.

Note: This survey deals only with Neustar's provision of NPAC services and not with any other services or products offered by Neustar. This survey resides on a secure third-party server hosted by TMNG, the firm hired to administer this process. Your individual responses will be held confidential and will not be shared with anyone outside of Neustar and TMNG. Please note: including comments with your ratings will be most beneficial in addressing any potential future service changes/enhancements.

The survey will keep track of your company's answers for each section, and these answers may be accessed and changed at any time up until the survey deadline of October 26, 2012.

Thank you for participating.

Your responses are appreciated.

4	3	2	1
Extremely Satisfied	**Somewhat Satisfied**	**Somewhat Dissatisfied**	**Extremely Dissatisfied**

1. Customer Service

1a. Responsiveness

	4	3	2	1
Help Desk—Tier 1 support				
Analysts—Tier 2 support				
Customer Connectivity Services				
Billing Personnel				
Account Management				
Senior Management				
Neustar overall				

Comments:

1b. Accessibility

	4	3	2	1
Help Desk—Tier 1 support				
Analysts—Tier 2 support				
Customer Connectivity Services				
Billing Personnel				
Account Management				
Senior Management				
Neustar overall				

Comments:

1c. Knowledge

	4	3	2	1
Help Desk—Tier 1 support				
Analysts—Tier 2 support				
Customer Connectivity Services				
Billing Personnel				
Account Management				
Senior Management				
Neustar overall				

Comments:

1d. Issues handled with a sense of urgency

	4	3	2	1
Help Desk—Tier 1 support				
Analysts—Tier 2 support				
Customer Connectivity Services				
Billing Personnel				
Account Management				
Senior Management				
Neustar overall				

Comments:

1e. Neustar personnel act as customer advocates

	4	3	2	1
Help Desk—Tier 1 support				
Analysts—Tier 2 support				
Customer Connectivity Services				
Billing Personnel				
Account Management				
Senior Management				
Neustar overall				

Comments:

2. Billing

	4	3	2	1
Accuracy				
Timely delivery				
Sufficient detail				
Ease of reading invoice				
Type of payment options				

Comments:

3. Industry forums (e.g. LNPAWG, Cross Regional, Testing)

	4	3	2	1
Knowledge level displayed				
Neutrality				
Responsiveness				
Documentation				
Use of resources				

Comments:

4. New Service Rollout

4a. On-time delivery of:

	4	3	2	1
SOW				
Product				
Level of Detail Description				
Schedule				
Pricing				

Comments:

4b. Testing

	4	3	2	1
Test Engineer Knowledge				
Test Engineer Responsiveness				
Test Engineer Communication Skills				
Applications Support Responsiveness to Issues				
Test Environment Availability for Scheduled Turn-up, Group and Failover Testing				
Test Engineer successfully managed testing time:				
o Turn-up testing				
o Group and Failover testing				

Comments:

5. Operations

5a. Outages

	4	3	2	1
Responsiveness of Help Desk, Service Delivery, Operations and Management				
Knowledge level of Help Desk, Service Delivery, Operations and Management				
Sense of urgency displayed by Help Desk, Service Delivery, Operations and Management				
Root Cause Analysis Reporting				
Accuracy of Resolution				

Comments:

5b. System Performance

	4	3	2	1
System Availability				
System Reliability				
System Responsiveness				
System Accessibility				
System Throughput				

Comments:

5c. Industry Communications

	4	3	2	1
Frequency				
Usefulness				
Timeliness				
Website content				
Website ease of use				

Comments:

6. NPAC Pool Block Provisioning and Mass Porting

	4	3	2	1
Accessibility of NPAC Pooling and Mass Porting personnel				
Responsiveness of NPAC Pooling and Mass Porting personnel				
Knowledge level of NPAC Pooling and Mass Porting personnel				
Order fulfillment - Timeliness				
Order fulfillment - Accuracy				
Ticket Support				
Issues handled with a sense of urgency				

Comments:

7. Neustar's Image as a vendor:

For the section that follows, please use the following definition as you provide your response:

- **Reliable**—Our clearinghouse services depend on complex technology that is designed to deliver reliability up to 99.9%. We commit to our customers to deliver high quality services across numerous measured and audited service levels, including system availability and response times.
- **Responsive**—We learn from the operational experiences of our customers and we routinely apply that knowledge to further enhance the clearinghouse. Our customers benefit from the compounded effect of shared industry insights.
- **Trusted**—The data we collect are important and proprietary. Accordingly, we have developed procedures and systems to protect the privacy and security of customer data, restrict access to the systems and safeguard the integrity of our clearinghouse.
- **Neutra**l—In managing our clearinghouse services, we adhere to FCC-defined neutrality regulations and policies. Independent third parties audit our adherence to these requirements on a quarterly basis. In fact, the FCC has designated Neustar as a neutral company.

	4	3	2	1
Neustar As Neutral Third-Party Service Provider				
Level of Trust your company has in Neustar				
Value Neustar brings to your company				
Neustar's Demonstrated Industry Thought Leadership				
Neustar's emphasis on technological innovation				
Neustar as a reliable partner				

Comments:

8. Overall customer focus

	4	3	2	1
Overall customer focus				

Comments: