Organization Security & Facilities Guidelines

Policy and Procedures

Last updated: Dec 2013

Document History and Version Control Table

Version No	Author	Effective Date	Change Summary
6.00	HR Team	Dec 2013	Personnel – Employee Responsibilities
5.00	HR Team	Jan 2013	Incidence Response Plan
4.00	HR Team	June 2012	Prohibited Activities
3.00	HR Team	Jan 2012	Execution of Request
2.00	HR Team	Feb 2011	Responsibilities assigned to security
1.00	HR Team	Jan 2010	Initial Version

Table of Contents

1. Physical Security Management 5

Categories of Security 5

1.1 Security of Restricted areas 5

1.2 Security of Assets 5

1.3 Security of personal information 5

1.4 Environmental security 5

1.5 Security of General areas 6

1.6 Responsibilities assigned to Security: 6

2. Organization Security - Space and Asset Movement Process 6

2.1 Guidelines for allocation of seats 7

2.2 Execution of Request 7

3. Information Security Policies 7

3.1 Summary of responsibilities 7

4. Network Security 8

4.1 User Accounts: 8

4.2 User Passwords: 8

4.3 Prohibited Activities: 9

5. Virus and Malware Controls 10

5.1 Recommended processes to prevent virus problems: 10

6. Incident Response Plan 10

Objective : 10

6.1 Incident Response Team (IRT) 11

6.2 Incident Response Team Members 11

6.3 Incident Response Team Roles and Responsibilities 12

6.4 Incident Response Team Notification 13

6.5 Breach of Personal Information - 13

6.6 Security Breach 14

6.6 a Requirements 14

6.6 b Data Owner Responsibilities 14

6.6 c Project Manager Responsibilities 15

6.7 When Notification Is Required 15

6.8 Incident Response – Breach of Personal Information 16

7. Personnel - Employee Responsibilities: 19

7.1 Guidelines to enter office 19

7.2 Employee Restrictions: 20

7.3 Issue of Temporary Pass: 20

1. Physical Security Management

The intent of Security guideline is to provide physical, data and materials security at all times and to create seamless and threat free work environment for employees. It also sets expectations from employees for smooth functioning of the process.

Categories of Security:

1.1 Security of Restricted areas

- Project Specific Areas
- Uninterrupted Power Supply Room
- Server Room
- AHU (Air Handling Unit)

1.2 Security of Assets

- All material assets belonging to NeoBytes Software Solutions
  Eg: Desktops, Laptops etc.

1.3 Security of personal information

- Directories and internal telephone extensions of NeoBytes and contact number of employees

1.4 Environmental security

- Fire alarms, smoke detectors
- Providing Fire Extinguishers and Fire Exits
- Use of heating, ventilation and air conditioning (HVAC) systems

1.5 Security of General areas

- Entry/Exit points
- Parking area

1.6 Responsibilities assigned to Security:

1. Ensure all employees swipe their access card
2. Stop any employee resorting to tail-gating
3. Check the Identity Card of every employee entering the facility
4. In the absence of the Identity card, employee will be asked to make an entry of time in the Register available with security
5. Assist in the implementation of Security measures
6. Tour the premises and report any untoward incidents to Admin
7. Supervise material movement into and out of the building
8. Ensure vehicles parking is in designated areas and in orderly manner. Check the parking area for any unauthorized parking and take actions immediately.
9. Assist the clients and visitors of NeoBytes Software Solutions during their visits
10. Assist various Managers during events held inside the building eg: Blood donation drive, Recruitment drive etc
11. Take head count of employees after the official hours and ensure that female employees leaving the office beyond the designated time have drop facility.
12. Coordinate with Building Security during visits and security related matters
13. Assist NeoBytes Admin during evacuation and other emergency situations
14. Provide periodic checks of all Panic Door Emergency Exits
15. Give daily reports as assigned to Admin Manager
16. Ensure proper discipline and decorum in the Reception area
17. Remain alert and observe the area for any smoke, smell, fire & impending danger
18. Should report to the Admin in case the access control doors are not functioning
19. Ensure that no vendor is allowed inside the secured project area without security escort or accompanied by Admin team person and proper authority
20. In case of fire raise an Alarm as per procedure
21. Ensure power supply is stable and inform Admin in case of any power
22. Ensure UPS and DG are in working condition

2. Organization Security - Space and Asset Movement Process

The objective of this process is to allocate space to employees as per Business needs and to enable internal office movement of assets in accordance to existing statutory regulations.

2.1 Guidelines for allocation of seats

1. Seats are allotted to Projects based on their current needs and projections
2. The allocated seats are contiguous to the present arrangement to enable proximity of all employees in the same Project but is solely based on availability
3. Secured bays allotted to Projects with security restrictions are not shared with other Projects
4. External vendors are not permitted to work in NeoBytes premises unless on special request by the clients and approved by Manager
5. Access to these vendors is restricted to the specific project work space allotted to them
6. Admin allocates seats based on the requests from Project Managers through "Issue Tracker" tool. Link : URL: http://nb-sep-server/nbit/home/index.dll
7. Admin will maintain the seating map

2.2 Execution of Request

- Admin will obtain approval from HR and allots seat in consultation with PM / Lead
- Network and System team will be looped to enable movement of items like desktops, phones, VPN etc. as per the request of PM / Lead.
- The SLA is as defined for the Admin Team and Network team to complete the movement is 24hours from the time of receipt of request.

3. Information Security Policies

The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the Organization or members of the Organization, and could also subject the Organization to fines or other government sanctions. Additionally, if Organization information were tampered with or made unavailable, it could impair the Organization's ability to do business. The Organization therefore requires all employees to diligently protect information as appropriate for its sensitivity level.

3.1 Summary of responsibilities

All employees and contractors

1. You may only access information needed to perform your legitimate duties as an employee and only when authorized by the appropriate approvals.
2. You are expected to ascertain and understand the sensitivity level of information to which you have access through training, other resources or by consultation with your manager.
3. You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the manager within the scope of your professional activities.

4. You must adhere to company’s policy for protecting any computer that is used for business and the computers used to transact the business regardless of the sensitivity level of the information held on that system.
5. You must protect the confidentiality, integrity and availability of the Organization's information as appropriate for the information's sensitivity level wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
6. Information deemed Confidential or Highly Confidential under this policy must be handled in accordance with the Organization's requirements for protecting Confidential and Highly Confidential information.
7. You must safeguard any physical key, ID card or computer/network account that allows you to access any internal information. This includes creating difficult-to-guess computer passwords.
8. Use of external USB drive or CD/DVD strictly prohibited and require prior approval from IT department.
9. You must report any activities that you suspect may compromise sensitive information to your supervisor or to the NeoBytes Network and IT Team.
10. Your obligation to protect sensitive information continues after you leave the Organization.
11. Personal Laptops/ Tablets are not allowed in the office premises.
12. Use of external USB port on the desktops and laptop are prohibited on any of the company’s laptops/desktops.

4. Network Security

User account is created when a person joins newly and his line manager would send in a request using issue tracker to create a user account. Authorization and Request needs to be approved for an active account.

4.1 User Accounts:

1. User accounts are assigned to individuals
2. Users shall not share their accounts
3. Users shall have full responsibility for the use of their account and will be held responsible for any policy violations that are traced to their account

4.2 User Passwords:

1. Users shall read and comply with the Password guidelines provided by Microsoft while you change the password.
2. Users shall access resources through the Internet/Intranet by using only those users IDs or methods that they have been authorized to use. Users shall not impersonate another

person, use pseudonyms or be anonymous when communicating via the Organization Internet/Intranet

3. Users shall not share their passwords, or record their passwords on hard disk drives, e. g. within Web browsers or mail programs, or in any other insecure location.

4.3 Prohibited Activities:

Users shall not engage in the following activities:

1. Illegal use of the Organization Internet/Intranet for any purposes which violate applicable laws, including, but not limited to disseminating, mailing, posting, receiving or solicitation for the reception of illegal material such as child pornography, obscene, threatening, intimidating or harassing material, or hate propaganda, in any form; making public to Organization or other users any such materials or direct links to such locations elsewhere on the Internet.
2. Use of the Organization Internet to libel or slander other users, individuals or institutions violation of copyright, trade secrets or infringement of any patent or other proprietary interest, including any activity that supports illegal distribution of software, otherwise known as pirating.
3. Gaining or attempting to gain unauthorized access to any kind of network, service, information, communications, or computing facility or resource through use of the Organization Internet/Intranet
4. Damaging/destroying the integrity of a computer system, or the data or programs stored on a computer system
5. For displaying, receiving or disseminating sexual or pornographic material, in any form, for personal or non-work-related use, regardless of the legality of the material.
6. For posting ads for money making schemes, including pyramid schemes.
7. Propagation of computer viruses, "worms", "Trojan horses" or other malicious code, including Virtual Viruses
8. Maliciously physically disabling a computer or computer components
9. Sending electronic chain letters or wide distribution e-mail
10. Wasting resources (human, network capacity, computer)
11. Making large numbers of article posts to inappropriate newsgroups (referred to as spamming)
12. Playing network based games
13. Attempting to monitor or tamper with another user's electronic communications, except for monitoring by security and systems administrators in the performance of their authorized duties.
14. Unauthorized publishing or distribution of official information; uploading, downloading, modifying, or removing files on any node in the network
15. Posting files or information to the World Wide Web, newsgroups, or ftp servers without authorization
16. Distributing or displaying material which is in any way inconsistent with Organization standards, community standards, or solicitation or reception of such material

17. Contacting software vendors, outside service vendors, outside network vendors, or any entity providing services or support to the Organization's computer and network system without express authorization of the Director

5. Virus and Malware Controls

5.1 Recommended processes to prevent virus problems:

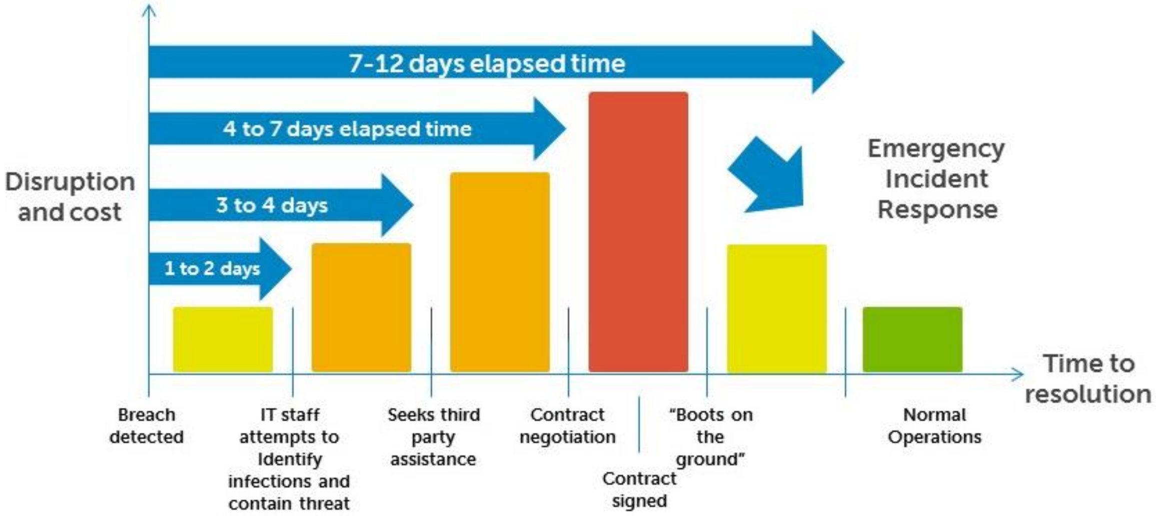
Always run the corporate standard, supported anti-virus software is available from the IT team.

1. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your recycle Bin. If you are still facing virus issues please bring it to the notice of Network and IT Team
2. Delete spam, chain, and other junk email without forwarding.
3. Never download files from unknown or suspicious sources.
4. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
5. Always scan any external media from an unknown source for viruses before using it.
6. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
7. If testing conflicts with anti-virus software, report it to IT team we will look into it.
8. New viruses are discovered almost every day. Periodically check the Anti-Virus Policy and this Recommended Processes list for updates

6. Incident Response Plan

Objective :

This plan outlines the steps to follow in the event secure data is compromised and describes the responsibilities of the Incident Response Team. The Incident Response Team (IRT) is expected to put the plan into action.



6.1 Incident Response Team (IRT)

The Incident Response Team is entrusted to offer a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Network Team will coordinate these investigations. The Incident Response Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents.

6.2 Incident Response Team Members

Each of the following members will have a primary role in incident response.

- Director
- Vice President

- IT Team

Network support members are expected to provide supporting roles during incident response.

6.3 Incident Response Team Roles and Responsibilities

IT Help Desk:

- SPOC for all computer incidents
- Notifies Sr. Network Admin and IRT team

IRT Team

- Sr, Network Admin determines play an active role in the investigation to understand the nature and scope of the incident
- Offers options to mitigate and contacts Director for advice
- Provides proper training on incident handling to help desk and IRT Team
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the incident and corrective action taken

Network Engineer

- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP)
    - port monitors, and event loggers
- Looks for signs of a firewall breach
- Contacts external Internet service provider for assistance in handling the incident
- Takes action necessary to block traffic from suspected intruder

Project Managers

- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the Network Team with any information relating to a suspected breach
- Collects pertinent information regarding the incident at the request of the Network Team

Windows Operating Systems Administrators

- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity

Internal Audit
Periodically reviews policies and procedures for compliance with information security standards.

6.4 Incident Response Team Notification

The Service Request Desk will be the central point of contact for reporting computer incidents or intrusions. The Service Request Desk will notify the Sr. Network Admin. All computer security incidents must be reported to the Sr. Network Admin. A preliminary analysis of the incident will take place by the Sr. Network Admin and that will determine whether Incident Response Team activation is appropriate.

6.5 Breach of Personal Information -

This Incident Response Plan outlines steps our organization will take upon discovery of unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a customer or employee of our organization.

In addition to the internal notification and reporting procedures outlined below, credit card companies require us to immediately report a security breach, and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Selected laws and regulations require the organization to follow specified procedures in the event of a breach of personal information.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an Individual or used to directly or indirectly identify an individual. Most information the organization collects about an individual is likely to be considered personal information if it can be attributed to an individual.

For our purposes, personal information is defined as an individual’s first name or first initial and last name, in combination with any of the following data:

1. Social Security number/Social Insurance Number
2. Driver’s license number or Identification Card number
3. Home address or e-mail address
4. Medical or health information

6.6 Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

6.6 a Requirements

Data owners must identify and document all systems and processes that store or utilize personal information on individuals. Documentation must contain system name, device name, file name, location, database administrator and system administrator (primary and secondary contacts for each). The business area and the IT development group must maintain the contact list of database and system administrators.

Likewise, all authorized users who access or utilize personal information on individuals should be identified and documented. Documentation must contain user name, department, device name (i.e., workstation or server), file name, location, and system administrator (primary and secondary contacts).

6.6 b Data Owner Responsibilities

Data owners responsible for personal information play an active role in the discovery and reporting of any breach or suspected breach of information on an individual. In addition, they will serve as a liaison between the company and any third party involved with a privacy breach affecting the organization’s data.

All data owners must report any suspected or confirmed breach of personal information on individuals to the Sr. Network Admin immediately upon discovery. This includes notification received from any third party service providers or other business partners with whom the organization shares personal information on individuals. The Sr. Network Admin will notify the appropriate administrator and data owners whenever a breach or suspected breach of personal information on individuals affects their business area.

> Note: For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the Service Request Desk will act as a central point of contact for reaching the Sr. Network Admin.

The Sr. Network Admin will determine whether the breach or suspected breach is serious enough to warrant full incident response plan activation. The data owner will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the Sr. Network Admin, throughout the investigation.

6.6 c Project Manager Responsibilities

Project managers are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting personal information.

If a breach or suspected breach of personal information occurs in their department, the department manager must notify the Service Request Desk immediately and open an incident report.

Note: Education and awareness communication will be directed to all employees informing them of the proper procedures for reporting a suspected breach of personal information on an individual.

6.7 When Notification Is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

a. A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.

b. An intruder has broken into database(s) that contain personal information on an individual.

c. Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing personal information on an individual has been lost or stolen.

d. A department or unit has not properly disposed of records containing personal information on an individual.

e. A third party service provider has experienced any of the incidents above, affecting the organization's data containing personal information.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the organization can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

a. The organization is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.

b. The organization determines that personal information on an individual was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.

c. An intruder accessed files that contain only individuals' names and addresses.

6.8 Incident Response – Breach of Personal Information

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

IT Help Desk

Contacts

Office Phone	080-41219394
E-Mail	<dattaraj.chandu@neobytes.com>

Primary: Dattaraj Chandu
Alternate: Ramesh Ekambaram – Sr. Network Admin

1. The IT Service Request Desk will serve as a central point of contact for reporting any

suspected or confirmed breach of personal information on an individual.

2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the IT Service Request Desk will open a Priority Incident Request.

3.The IT Service Request Desk advises that a breach or suspected breach of personal information on an individual has occurred. After that Sr. Network Admin analyzes the facts.

Sr. Network Admin

Contacts

Office Phone	080-41219394
E-Mail	ramesh.ekambaram@Neobytes.com
Primary:	Sr. Network Admin
Alternate:	**Director**

1. When notified by the Service Request Desk, the Sr. Network Admin performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.
2. Informs the Director that a possible privacy breach has been reported and provides them an overview of the situation.
3. Contacts the individual who reported the problem.
4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of personal information about an individual. (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).
5. Reviews the preliminary details with the Sr. Network Admin.
6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the Service Request Desk and advise them to update the Incident Request with “Incident Response Team Activation – Critical Security Problem”.
7. Notify the Public Relations Department of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.
8. The IRT is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.
9. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.
10. Contact appropriate Incident Response Team members and First-Level Escalation members.
11. Identify and contact the appropriate Data Owner affected by the breach. In

coordination with the Vice President, the Sr. Network Admin and Data Owner, determine additional notification requirements (e.g., Human Resources, external parties).

12. If the breach occurred at a third party location, determine if a legal contract exists. Work with the Business Office, the Security Manager and Data Owner to review contract terms and determine next course of action.
13. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.
14. If personal information is involved, have the Data Owner determine who might be affected.
15. Determine if an intruder has exported, or deleted any personal information data.
16. Determine where and how the breach occurred. Identify the source of compromise, and the timeframe involved. Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected. Look at directory and file permissions. Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
17. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls. Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account. Do not access or alter the compromised system. Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
18. Monitor systems and the network for signs of continued intruder access.
19. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation. Note: Visa has specific procedures that must be followed for evidence preservation.
20. Notify the Vice President and Administration as appropriate. Provide a summary of confirmed findings, and of the steps taken to mitigate the situation.
21. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary action and possible termination. In the case of

contractors, temporaries, or other third-party personnel, ensure discontinuance of the user’s service agreement with the company.

Human Resources

Contacts

Office Phone	080-41219394
E-Mail	Thejaswini Kulkarni <thejaswini.kulkarni@neobytes.com>
Primary:	**Thejaswini Kulkarni**

1. If notified of a privacy breach affecting employee personal information, open an incident request with the IT Service Request Desk to activate the Incident Response Plan for suspected privacy breach.

2. When notified by the Sr. Network Admin that the privacy breach incident response plan has been activated for a breach of information on an individual, perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.3. Work with the IT Service Request Desk, Sr. Network Admin and business area to identify the extent of the breach.

4. If appropriate, notify the business area that a breach has been reported and is under investigation.

5. Work with the business area to ensure there is no further exposure to privacy breaches.

6. Work with the Sr. Network Admin and Legal Department to determine if the incident warrants further action.

7. Personnel - Employee Responsibilities:

7.1 Guidelines to enter office

1. Swipe Access card and Finger Print detector at every entry/exit
2. Display of Identity card in the premises at all times
3. Disclose personal belongings for security check at every check-in and check-out
4. Responsible for the safety of personal as well as company assets provided to employee
5. Clearance of desk when away from workstation
6. Report to Admin Team /Security immediately in case of any incidents
7. Adhere to all security checks organized by the building security
8. Familiarize themselves with the Facility for emergency evacuation
9. Ensure entry of personal visitors is restricted to Reception area
10. Collection of vehicle stickers to avail parking at NeoBytes parking area
11. Parking slots are available to employees on first-come, first-served basis

12. Affix the vehicle sticker on the vehicle (vehicles without the parking sticker will not be allowed entry to the parking area)

7.2 Employee Restrictions:

1. Bringing into the office premises any personal electronic media
2. Bringing in personal camera into the office premises
3. Photography, unless prior approval from Admin is obtained

7.3 Issue of Temporary Pass:

- Admin issues Temporary Access cards to employees
- Employee has to return the Temporary access card to Security the same day
- In case the above temporary access card is not returned the same day, employee access card will be de-activated by Admin Team with immediate effect
- Availing Temporary access cards for more than 3 consequent days and more than twice in a month is not allowed