1 800 388 4264
nrchealth.com

Information Security Policy Overview

Coverage

This policy applies to all NRC Health Associates, clients, contractors, partners, and temporaries who use NRC Health computing or networking resources.

Policy

Compliance with this policy is mandatory. NRC Health and client information exists in many forms and is an important business asset that has value to the company and our clients. Information can be printed, written, stored electronically, spoken in conversation, shown on video and transmitted by through use of paper documents or electronic means. Whatever the medium, information should always be properly protected from the time of its creation, through its useful life, and until its authorized disposal.

As with other assets, not all information has the same use or value and therefore systems and processes must be used to define the level of protection required based on the information's confidentiality, integrity and availability characteristics.

- *Confidentiality* – Levels of authorization and authentication required to access to the information
- *Integrity* – Controls over the accuracy and completeness of information and processing methods
- *Availability* – The ability for authorized users to have access to information and associated assets when required

Each authorized user of NRC Health information has an obligation to preserve and protect the security and privacy of information in a consistent and reliable manner. Security controls provide the necessary physical, logical, and procedural safeguards to accomplish those goals.

This policy states minimum requirements and defines responsibilities for meeting NRC Health's information security objectives.

Organizational & Functional Responsibilities:

Management: Senior management is fully committed to information security. Their responsibilities include:

- Establishing the guiding principles and objectives for the information security program.
- Appointing a qualified **Director of Information Security** for the organization.
- Establishing, reviewing and approving an information security policy for the organization.
- Ensuring that the information security policy is communicated to all Associates.
- Providing resources required for establishing and maintaining the information security program.

Director of Information Security: The **Director of Information Security** is responsible for administration of this policy. Duties include:

- Providing direction to and overseeing the activities of the Corporate Security Analyst and Corporate Security Engineer.
- Developing and maintaining hardware and software standards and procedures necessary to ensure implementation of and compliance with this policy
- Ensuring appropriate security requirements for user access to automated information systems are defined
- Providing support and guidance to Associates in fulfilling their responsibilities by implementing a Security Awareness Program that explains the issues, why policies have been established, and what roles individuals have in safeguarding information
- Providing frequent updates to Associates and senior management on emerging security threats and control measures that should be implemented to mitigate risks
- Monitoring significant changes in legal or regulatory requirements and providing updates to senior management
- Reviewing and monitoring information security incidents, insuring corrective actions including implementation of additional compensating controls are initiated, and reporting the findings and corrective actions to IT Management
- Reviewing and approving all external network connections to NRC Health's network
- Assisting with maintenance of NRC Health's Business Continuity Plan to ensure the continuity of NRC Health's business and security controls

- Reviewing new applications and services to assess security threats and ensure appropriate security process are implemented

- Serve as NRC Health's HIPAA Security Officer

IT Management: IT management has responsibility for the data processing infrastructure and computing network. It is the responsibility of IT management to:

- Develop, deploy, and maintain an information security architecture that will provide the range of security controls required to provide an appropriate level of protection based on the information's confidentiality, integrity and availability characteristics

- Ensure that critical data is backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when it is needed

System Owners: Individuals serving as System Owners or Data Stewards must:

- Classify information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery

- Determine the type of access privileges that should be granted (inquiry, update, etc.) to ensure protection of information and adequate separation of duties

- Determine who should have access to protected systems within their jurisdiction

- Conduct quarterly reviews of Associate access rights to ensure privileges are consistent with current job responsibilities

Managers: Managers and supervisors must:

- Ensure that all Associates are aware of and comply with this policy

- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all associates observe this policy

- Promote the importance of the Information Security Program throughout the organization

- Report security incidents immediately to the **Director of Information Security**

Associates: Associates must:

- Read and comply with established information in the NRC Health's Code of Conduct, the Acceptable Use Policy, and the Information Security Flyer provided during new hire orientation and posted on the Intranet

- Only access information to which they are authorized and safeguard the confidentiality of information

- Ensure that log-on and passwords used to identify and authenticate users are not disclosed or shared

- Report security incidents immediately to the **Director of Information Security**

Risk Assessment and Evaluation

At least annually, The **Director of Information Security** provides the results of a risk assessment to the leadership team along with an action plan to address any shortcomings across NRC Health's security, privacy and compliance risk spectrum. This risk assessment shall be deemed confidential and privileged, and is not to be shared with customers as it contains risk out of scope to individual applications and customers.

There are three main factors that must be considered when preparing recommendations:

1. Objectives and requirements for information processing in supporting operations should be restated and reaffirmed.

2. Recommendations must be based on the likelihood of a security failure and proposed expenditures must be balanced against the potential damage likely to result from security failures.

3. Changes in legal, regulatory and contractual requirements for the organization, clients, partners, contractors and service providers must be evaluated to ensure continuing compliance.

As part of the assessment, the NRC Health's Leadership Team will be notified on progress of mitigating existing threats and of any new threats that could significantly increase the risk to the company.

The Director of Information Security, assisted by the Corporate Security Analyst shall maintain a risk register documenting high and critical risks that take longer than thirty (30) days to remediate, and shall share the risk register with NRC Health's executive leadership at least quarterly along with the current status of plans to mitigate, remediate and cure such risks.

Education and Training

The foundation of an effective security program is the education and training of all associates and, where relevant, third party users (clients, vendors, contractors, etc.). An Acceptable Use Policy and an Information Security Flyer is provided to all associates during new associate orientation.

The information covers security requirements, legal responsibilities and business controls, and the correct use of information processing resources e.g. password and log-on procedures, authorized use, trouble and incident reporting.

Email notifications are also provided to inform associates of current threats and preventative measures.

Physical Security

Breaching physical security can cause a loss of or damage to NRC Health's information. It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. All central processors, networked file servers, central network equipment, and wiring closets for network and telephonic connections will always be located in a Data Center with restricted access controlled through key access.

Access to the Data Center is restricted to designated staff, whose job function requires access to equipment in the Data Center. Clients and authenticated representatives of third party support agencies are only given access through authorization from the Director of Information Security or staff with access to the Data Center. Clients and representatives of third party support agencies must be escorted at all times during their work in the Data Center and must sign in on the Data Center Visitor Log.

There is also a risk of disclosure through careless disposal or re-use of equipment. Formal processes have been established to minimize this risk. Storage devices such as hard disk drives and other media (e.g. tape, CDs, DVDs, cell phones, digital copiers or other devices that store information) or paper containing Company information must be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information.

Manager Responsibilities

- Assign appropriate levels of facility and systems access for all associates, contractors, and guests
- Contract with bonded service providers for data storage and destruction of electronic media and paper documents

Associate Responsibilities

- Visitors must be escorted at all times within the facility
- Access cards or keys must not be shared or loaned to others and lost or stolen access cards or keys must be reported to Security immediately
- Special care must be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of NRC Health's premises to prevent persons from viewing or accessing information
- Associates are responsible for the security of devices issued to them. Laptops, handheld computing devices (i.e. Smart Phone's, Portable Tablets), and removable storage media (i.e. disks, tapes, USB devices…etc.) must be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be password locked and

encrypted. While travelling, associates should lock laptops in car trunks if otherwise unattended and not in use.

- Removable storage media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided
- Request the IT department to assist with all equipment installations, disconnections, modifications, and relocations. This does not apply to temporary moves of portable computers for which an initial connection has already been set up by IT
- Shred documents with confidential information **or** place documents in bins for shredding and re-cycling
- Exercise care to safeguard electronic assigned computing or communication equipment. Associates may be accountable for any loss or damage to assigned equipment

Systems Planning, Development, Acceptance and Maintenance

NRC Health has standardized its server environment on the windows platform and Linux operating systems to better service our corporate needs. All servers have their systems clock synchronized with one of the atomic clocks.

Security is considered in all systems planning, development, acceptance, and maintenance activities. Each new development project includes a section on security and all development requires IT and user acceptance testing. Separation of the development, test, and production environments is also required, either logically or physically. To minimize the possibility of corruption of information systems, strict controls over changes have also been implemented.

All server installations must also follow Server Hardening procedures that include:

- Installation of the operating system from a reliable source
- Application of vendor supplied fixes
- Removal of unnecessary software, system services, and drivers
- Setting of security parameters, file protections and enabling of audit logging
- Disabling or changing passwords associated with default accounts
- Installation of appropriate intrusion detection and/or file integrity software

To reduce the risk of accidental or deliberate system misuse, separation of duties or areas of responsibility are implemented where practical. Whenever separation of duties is difficult to

achieve, other compensatory controls such as monitoring of activities, audit trails and management supervision are implemented.

Applications and systems are reviewed periodically to insure adequate control measures are in place. Storage and memory capacity demands are also monitored and future capacity requirements are projected to ensure adequate processing and storage capability is available when needed.

Each system has a scheduled maintenance plan to include a log of hardware and software upgrades, patches and fixes. Security bulletins are reviewed by IS operations at least weekly to insure that all known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the risk of security incidents that could affect the confidentiality, integrity and availability of business data or software integrity.

Virus protection software must be installed on all NRC Health computers running operating systems traditionally affected by viruses and malware and must be automatically registered with NRC Health antivirus servers. Email gateways also utilize properly maintained email virus protection software. Virus signature files are also updated daily or when the virus software vendor's signature files are updated and published.

All production servers are on an appropriate backup schedule. All client and controlled corporate data is retained in accordance with contracted agreement or by law. Other data is retained based on local system policy. Destruction or return of client data is performed in accordance with client contract/agreement.

IT Responsibilities

- Monitor storage and memory capacity demands to ensure adequate capacity too meet business needs
- Complete all required maintenance and ensure all patches and fixes are installed on a timely basis
- Conduct and maintain records of all IT testing of new applications or enhancements
- Ensure all backups are executed according to the back up schedule
- Install and maintain appropriate antivirus software on all computers
- Respond to all virus attacks, destroy any virus detected, and document each incident

Manager Responsibilities

- Ensure appropriate associates are available to conduct required user acceptance testing
- Ensure adequate separation of duties in departmental reorganizations and designs of new applications or application enhancements

Associate Responsibilities

- Participate in user acceptance testing
- Do not knowingly introduce a computer virus into company computers
- Do not load magnetic media or programs of unknown origin and scan all magnetic media for viruses before they are read
- If a workstation appears to have been infected by a virus, IMMEDIATELY POWER OFF the workstation and call the Help Desk

Information Access and Passwords

Computer equipment must be physically protected from security threats and environmental hazards and the confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized associates have access.

Controls have been implemented to require authentication on desktops, laptops, and any other computer systems to ensure that access is restricted to only those capabilities that are appropriate to each associate's job duties. Additional controls include password protected screen savers, automated logoff processes, and re-authentication after a set time out period. The issuance and use of privileged accounts is limited to authorized persons within the IT department.

Only network addresses issued by NRC Health's Network Administrator may be used on NRC Health's network.

To ensure that systems meet minimal acceptable guidelines for compatibility and security, the Director of Information Security must also approve the use of any computer systems that is not owned by NRC Health before it can be attached to NRC Health's network.

All access to any of NRC Health's networks by external parties must also be authorized by the Director of Information Security. No network hardware (router, switch, but, firewall, wireless access point, or other network appliance) may be installed on NRC's networks without approval from the Director of Information Security. Arrangements involving third parties must include or consider the following:

1. A description of services to be performed (including any involvement of additional subcontractors) with definitions of acceptable and unacceptable levels of service
2. Agreement on NRC Health's right to audit contractual responsibilities or have audits conducted by a third party
3. A definition of responsibilities with respect to data protection that includes:
    - Agreement to sign security and confidentiality agreements
    - Adherence to legislative or regulatory requirements in respective states and or countries
    - Facility and system access control agreements stating NRC Health's right to monitor and revoke access
    - Restrictions on copying and disclosing information
    - Definition of processes for reporting and investigation of security incidents
    - Requirements for controls to ensure protection against malicious software
    - Procedures to determine whether a compromise of the assets (i.e. loss or modification of data) has occurred
    - Controls to ensure the return or destruction of information and assets at the end of a contract or agreed upon point in time during the contract
4. A clear reporting structure that includes any provisions for transfer of staff
5. A description of responsibilities regarding hardware, software installation, cabling, maintenance, and any requirements for user and administrator training in methods, procedures, and security
6. A description of an escalation process for problem resolution
7. Agreement on a change management process
8. Definition of intellectual property rights, copyrights and protection of any collaborative work
9. A definition of respective liabilities of the parties to the agreement

Once third party access is granted, NRC Health's IT staff must control all external access to its systems by enabling and disabling connections for each approved access requirement.

IT Responsibilities

- Set all protocols and standards used on NRC Health's networks
- Install and maintain appropriate network firewalls

- Maintain a reliable network with as much built-in redundancy as is feasible
- Enable audit logs of firewall, network, server, and application access attempts
- Ensure all accounts with elevated priviledge must use two factor authentication.
- The Network Administrator is responsible for the administration of access controls to all company computer systems. The Network Administrator will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor
- The Director of Information Security is responsible for insuring appropriate agreements are in place and that training has been provided prior to granting access to company systems
- The Network Administrator is responsible for installing protected screen savers on user systems and sessions on production systems.
- The Network Administrator is responsible for setting policies to automatically terminate sessions if system specific session termination time periods elapse without user activity
- The Network Administrator is responsible for setting policies to force passwords to be reset on initial use of assigned temporary passwords
- The Network Administrator is responsible for setting policies to force password changes every 90 days with restrictions that prohibit the use of previously used passwords for five cycles unless exceptions are approved by the Director of Information Security
- The Network Administrator is responsible for setting policies to lock out accounts after 5 unsuccessful login attempts whenever possible. Note: Associates and Clients contact the Service Desk to request password resets if they are locked out of their systems. The Service Desk is responsible for verifying Associate and Client identity before performing the reset.
- The Network Administrator is responsible for disabling of accounts if individuals are on extended leave or accounts have not been accessed within 45 days
- The Network Administrator is responsible for changing associate passwords for a shared administrator/special access account when any individual knowing the password changes their role or terminates their association with NRC Health
- The Network Administrator is responsible for changing client passwords upon client request or termination of the relationship
- The Network Administrator is responsible for establishing special access accounts needed for auditing, software development, software installation, or other defined needs. These special access accounts must be:

- Authorized by the Director of Information Security
- Created with an expiration date.
- Removed when work is complete.

Manager Responsibilities

- The CFO or division president ensures that appropriate security, confidentiality and non-disclosure agreements are obtained from all contractors.
- Managers and supervisors must use public forms whenever an associate starts, leaves the company or transfers to another department so that Service Desk tickets are opened to ensure that access rights can be updated on a timely basis. Involuntary terminations must be reported concurrent with the termination
- Managers and supervisors must notify the Director of Information Security when a contractor is on site and needs access to systems

Associate Responsibilities

- Create a password that can be remembered, but is hard for anyone else to guess. Passwords should:
- Be at least eight (8) characters in length - the longer the better. (Passwords for Microsoft Windows® can be up to 128 characters long.)
- Include upper and lower case letters, numerals, symbols. Consider creating a password from a phrase. Instead of using a memorable word, choose a memorable event in your life and convert it to a secret code. For example: "I went to Ft. Lauderdale in 85!" would translate to: IwtF.Li85!
- Have at least one special character or base number (0-9) in the second through sixth position
- Have at least four different characters with no repetition of the same character
- Look like a sequence of random letters and numbers
- When creating a password, do not use:
- ANY PART of your logon name for your password
- Any actual word or name in ANY language
- Numbers in place of similar letters
- Any portion of your old password

- Consecutive letters or numbers like "abcdefg" or "234567"
- Adjacent keys on your keyboard like "qwerty"
- Manage passwords
- Do not write passwords down
- Do not share passwords. If there is a business reason to tell someone your password, create a new password as soon as possible
- Do not check the "remember my password" feature
- Create different passwords for highly confidential information
- Change your passwords at least every 90 days
- Contact the Service Desk for password re-sets if locked out of systems
- Log out when leaving a workstation for an extended period

Communications and Network Management

All NRC Health networks have appropriate security controls to ensure the integrity of the data flowing across these networks. In most cases, the security confidentiality requirements of the data being shared will determine the level of security required when sharing data. If there is a business need, additional measures to ensure the confidentiality of the data will also be implemented.

The Director of Information Security ensures that measures are in place to mitigate any new security risks created by connecting the NRC Health networks to a third party network. Where NRC Health has outsourced an application to a third-party service (such as web applications), the Director of Information Security performs periodic security reviews of the outsourced environment to ensure the security and availability of the NRC Health's information and application.

Protected Heath Information routinely flows between NRC Health's clients and within the company. The routine use of patient identifiable information could have an adverse effect on the client/patient relationship. It could also infringe individuals' rights to have confidential information about them used properly. With this in mind, NRC Health has established a privacy policy to ensure that the flow of patient identifiable information is appropriately controlled.

- Use and transfer of protected health information will only occur when absolutely necessary and with client and the responsible health care entity (information owner) approval
- Where possible, all data will be de-identified

- All associates are informed of HIPAA and security requirements and must understand and comply with the HIPAA Security and Privacy rules.

For information to be released outside of NRC Health, a process has been established that, at a minimum:

- Evaluates and documents the sensitivity of the information to be released or shared
- Identifies the responsibilities of each party for protecting the information
- Defines the minimum controls required to transmit and use the information
- Records the measures that each party has in place to protect the information
- Defines a method for compliance measurement
- Provides a signoff procedure for each party to accept responsibilities
- Establishes a schedule and procedure for reviewing the controls

Public Key Infrastructure (PKI), Digital certificates, and Secure Socket Layer (SSL) certificates are used for encryption of transmissions.

All NRC Health computing systems that provide information through a public network, either directly or through another service that provides information are also subjected to intrusion testing to determine if:

- An individual can make an unauthorized change to an application
- A user may access the application and cause it to perform unauthorized tasks
- An unauthorized individual may access, destroy or change any data
- An unauthorized individual may access the application and cause it to take actions unintended by the application designer(s)

NRC Health has implemented a multi-layered security model. Firewalls interface with each segment to control access and isolate production systems and sensitive data from outside intruders. NRC Health's networks must support and implement least privilege as the ability to view a device over a network port is the ability to attack that device, service and data stored.

NRC Health also deploys a state-of-the-art Intrusion Detection System (IDS) to actively monitor all nodes on NRC Health's corporate network. The intrusion detection system creates audit logs and provides alerts for high risk threats.

An independent vulnerability testing service has also been retained to run monthly testing to identify and report vulnerabilities in NRC Health's network to the Director of Information Security. The third party independent service conducts monthly probes of all secured and

unsecured web ports on NRC Health's Internet facing systems using known vulnerabilities. Any deficiencies are risk rated on a scale of 1 to 4 and a report of deficiencies is provided to the IT management. Threats of Level 3 or higher are deemed high or critical and are escalated to the Director of Information Security and must be repaired by the end of the day to maintain "Hacker Safe" certification. Critical and High vulnerabilities must be cured within fifteen (15) and thirty (30) days respectively.

The tools used to perform the vulnerability testing are updated to ensure that recently discovered vulnerabilities are included in any testing. The results of intrusion testing are reviewed in a timely manner by the Director of Information Security, and any vulnerability detected is evaluated for risk and mitigated as appropriate.

In addition to vulnerability testing, NRC Health shall conduct third party penetration testing using certified, trusted information security professionals at least once per year. Only individuals authorized by the Director of Security will perform penetration testing.

No client or agent of a client will be permitted to conduct its own security testing of NRC Health shared resources, as there are no systems or databases set aside for single customers. Before such testing could occur, each and every customer in scope to the relevant network, application and product would need to provide prior written consent, and potentially a HIPAA business associate agreement with the testing entity to avoid breach.

Acceptable use

It is the policy of NRC Health to provide Associates with the electronic communication systems (voice mail, electronic mail, operating systems, secure FTP, etc.), software, and computing equipment and storage media to assist in performing assigned job functions.

Access to the Internet is provided to associates as a productivity enhancement tool by allowing associates to connect to a variety of business information resources around the world.

NRC Health has developed an Acceptable Use Policy to provide guidelines that will protect NRC Health's Associates, Clients, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Associates are asked to sign the Acceptable Use Policy during new hire orientation.

Associate Responsibilities

- Ensure that all communications are for professional reasons and that they do not interfere with productivity
- Be responsible for the content of all text, audio, or images that they place or send over the Internet. All communications should have the associate's name attached
- Not transmit copyrighted materials without permission

- Know and abide by all applicable NRC Health policies dealing with security and confidentiality of company records
- Run a virus scan on any executable file(s) received through the Internet
- Avoid transmission of nonpublic client information. If it is necessary to transmit nonpublic information, associates are required to take steps reasonably intended to ensure that information is delivered using the appropriate security controls outlined in this document to the proper person who is authorized to receive such information for a legitimate use

Asset management

In an effort to provide adequate security controls and lower the total cost of ownership, NRC Health has implemented use of hardware standards for servers, desktops, laptops, laptop accessories, and printers.

Software standards have also been established and have been used in developing a laptop and desktop images for use in configuring all new or replacement systems.

An inventory of assets helps to insure that adequate protection of information and continuity of business. Information assets are broken down into four categories:

1. *Information Assets*: Databases, files, manuals, documents, removable media
2. *Software Assets*: application software, system software, development tools and utilities
3. *Hardware Assets*: computer equipment (processors, monitors, laptops,), communications equipment (routers, switches, hubs, wireless access points, internal cabling), other equipment (printers, fax, projection devices)
4. *Services*: computing and communication services, general utilities, heating, lighting, standard and emergency power (generator, UPS), air conditioning.

IT Responsibilities

- Provide a sufficient number of licensed copies of software to enable associates to perform their work
- Ensure installation of software complies with license agreements of the software and maintain proof of purchase and/or the original installation media for each software package
- Maintain records of software licenses owned by NRC Health and a list of authorized software, additions/changes and deletions approved by the Director of Information Security.

- Periodically (at least annually) scan company computers to verify that only authorized software is installed and remove software without proof of license
- Install, modify and repair assets in support of the companies business and security objectives
- Inventory information assets on an annual basis and report discrepancies to the Director of Security

Manager Responsibilities

- Safeguard the assets assigned to direct reports
- Notify the service desk of any changes in assignment or loss of hardware and software assets
- Enforce the established guidelines for modification of hardware and software assets by notifying the help desk when changes are required to support business needs

Associate Responsibilities

- Safeguard assigned computing or telecommunication assets and immediately report the loss of any assigned equipment to their manager
- Only software that is licensed to or owned by NRC Health is to be installed on NRC Health computers unless approved in writing by the Director of Information Security.
- Copying software is prohibited unless authorized. Associates must gain written approval from their managers and the Director of Information Security to download items not listed as approved freeware or NRC Health property.
- With written approval, request Service Desk assistance for loading software or modifying hardware

Intellectual Property Rights

NRC Health and its associates are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose NRC Health and the associate(s) to civil and/or criminal penalties.

Associates are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the company and/or legal action by the copyright owner. This policy applies to all software that is owned by NRC Health, licensed to NRC Health, or developed using NRC Health resources by associates or vendors.

Violations of copyright law expose the company and the responsible associate(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

Violations of copyright law that are committed “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)),” expose the company and the associate(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the company and may be regarded as public information. NRC Health reserves the right to access the contents of any messages sent from its facilities or via its company owned infrastructure if the company believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Security Incident Management

A security incident is an event which may result in:

- Degraded system integrity
- Loss of system availability
- Disclosure of confidential information
- Disruption of activity
- Financial loss
- Legal action
- Unauthorized access to applications

Because testing system weaknesses could have unintended consequences, associates and contractors must not attempt to prove a suspected weakness unless authorized by the Director of Information Security.

All NRC Health staff and contractors are required to report any observed or suspected incidents by opening a Service Desk Ticket as quickly as possible and are asked to record the symptoms of the problem and any messages displayed. Once an incident has been identified, IT staff:

- Identify the underlying cause of the incident and provide notification to other affected users if appropriate
- Immediately report all security incidents that may have an impact on the company to the Director of Information Security
- Identify procedures that will be employed to resolve the problem and if appropriate, isolates the affected system, and stops use of the system until the problem has been identified and resolved
- Escalate the incident if it cannot immediately be resolved
- Identify procedures that will be employed to prevent the same or similar incident from occurring

IT tracks the response process from initial report to resolution through updates to the Service Desk Ticket. Closure of the Service Desk ticket notifies the person who reported the incident of what took place and how the incident was resolved.

The IT Manager reviews the types and volumes of security incidents and malfunctions to identify recurring or high impact incidents and to record lessons learned.

Associate Responsibilities

- Ensure that no actual or potential security breaches occur as a result of associate actions. Security breaches may result in disciplinary action.

Business Continuity Management

NRC Health has developed a Business Continuity Plan that is reviewed and updated on an annual basis.

IT Responsibilities

- Technical staff from the Incident Response Team are responsible for working with vendors to ensure that any damage from a security incident is repaired or mitigated and that the vulnerabilities are eliminated or minimized

Manager Responsibilities

- Ensure associates are aware of responsibilities defined in Departmental Addendums
- Assist Incident Response Teams in identifying and documenting risks and recommended Action Plans

Violation/Enforcement

Violations of this policy can lead to revocation of system privileges and/or disciplinary action up to and including termination. Suspected violations should be reported immediately to supervisors, managers, or the Manager of Information Technology to ensure prompt, proper, and consistent investigations and responses.

If it is determined that an Associate or representative has misappropriated or misused NRC Health assets, NRC Health may pursue legal remedies against the Associate or representative to recover the asset or obtain compensation for damages.

Questions about this policy or requests for approvals of exceptions to this policy should be directed to the Director of Information Security or emailed to security@nationalresearch.com.

Revision History

Date of Change	Responsible	Summary of Change
09/20/2012	Director of Information Security	Policy established
06/01/2014	Corporate Security Analyist	Annual review
06/25/2015	Corporate Security Analysit	Annual Review
06/20/2016	Corporate Security Analyist	Annual Review
05/01/2017	Director of Information Security	Formatted for new brand Included Corporate Security Engineer position
8/1/2017	Director of Information Security	Added two-factor authentication required for all users with elevated priviledge.
4/17/2018	Corporate Security Analyst	Annual Review
8/14/2018	Director of Information Security	Gramatical and rebranded errors