Information Security Overview

Version 3.0, August 2007

Submitted by:	Paul Lagacey, Vice President – Information Security
Address:	NCO Financial Systems 507 Prudential Road Horsham, Pennsylvania 19044
Phone Number:	(800) 220-2274, ext. 3028
Cell Number:	(215) 384-4057
E-mail Address:	Paul.Lagacey@ncogroup.com

Table of Contents

Corporate Information Security Overview

The security and confidentiality of client and customer information is of the utmost importance to NCO management and individual employees. As such, we employ a variety of technical and non-technical measures of mitigating risk including firewalls, encryption, access controls, permissions, and physical site security to ensure customer data remains secured per NCO policy, standards, and requirements.

NCO works diligently to meet or exceed customers' data privacy and security needs, in addition to implementing industry standards, and regulatory and fiduciary requirements, in order to prohibit the possibility of an information compromise.

NCO uses a multilayered methodology to secure our clients' information, so that we may provide a holistic approach to data protection. The measures we employ include but are not limited to:

- Corporate-wide policies, procedures and standards for data protection encompassing both business functionality and Information Technology solutions
- Dedicated information and physical security staff responsible for centralizing and managing physical and logical controls
- Disaster recovery and business continuity planning and yearly testing
- User access on "need-to-know" basis according to job function
- Physically segregated work areas based upon roles and responsibilities
- Security patch management
- Security hardening specifications
- Preventive intrusion detection and prevention system
- Perimeter security, redundant border routers and firewalls
- Vulnerability alert tracking and response
- Weekly vulnerability assessments of critical systems
- Quarterly third-party external compliance scans
- Annual third-party "ethical hacking" testing on critical systems

Information Security Policy and Procedures

The systems and security measures described in this document are active components of, and adhere to, NCO's security and privacy policies and procedures that are integrated into our business operations.

Our systems and security architecture have been based upon industry standards, customer needs, and regulatory requirements. These standards and requirements are regularly reviewed and revised for use in connection with NCO's business solutions.

Our corporate information security policy and procedures define standards for administrative, technical, and physical safeguards. These documents are available for onsite review and discussion, upon request, on a case-by-case basis.

Site Security

Access to NCO facilities is restricted by role and responsibility. Various combinations of locking devices, keypads, card-controlled access, facial recognition mechanisms, cameras, security lighting, alarm systems, and 24-hour guard services are used to restrict access and monitor critical facilities, such as our corporate data center. Multi-tenant buildings use contracted guard services as arranged by the building manager.

Data Security

NCO maintains data security by limiting access to program-specific data to IT and non-IT personnel on a need-to-know basis. Based on management approval, NCO assigns specific system and application level credentials to personnel. In addition, administrative access to sensitive information and/or applications may be controlled via two-factor authentication, when deemed necessary, on a project, customer, or application basis.

Hard copy data, CD-ROM, and back-up tapes are archived offsite in a secure environment. Documents and electronic media no longer needed are shredded, destroyed, or erased, per Department of Defense specifications.

NCO's internal auditors oversee the integrity and effectiveness of our data security procedures, policies, and practices to ensure their continued effective implementation.

Firewalls and Encryption

NCO uses advanced firewall technology to enforce secure access between our internal networks, the Internet, customers, and partners. NCO supports industry-standard encryption, in addition to virtual private network (VPN) technology to ensure data integrity and confidentiality. In an effort to mitigate common security concerns, NCO leverages multiple vendors to provide core security products such as firewalls, network layer devices, and intrusion detection and prevention systems. Logging is enabled on critical systems allowing NCO to consolidate and correlate corporate-wide

activity via an information security event monitoring and correlation system. This system positions NCO to monitor and mitigate potential threats, vulnerabilities, and security concerns.

Firewalls, dedicated VPN appliances, and routers are deployed using a robust, built-in encryption schema permitting proprietary site-to-site and remote access via secured solutions. Enterprise-wide firewall protection in a multi-tiered deployment enables concealment of the NCO network architecture from the outside world and helps reduce the risk of external parties accessing our core network.

NCO strongly encourages our clients to encrypt their data for transfer to and from NCO, per our approved encryption standards. NCO is capable of accommodating several standard types and levels of encryption required by a client.

Detection and Monitoring

NCO uses an intrusion detection/prevention system to monitor and alert the appropriate IT personnel upon occurrences of potential threats to our critical systems. Our host systems maintain detailed audit logs of access, whether authorized or unauthorized, and are reviewed by the information security department. An information security monitoring and correlation system is currently deployed enabling NCO to effectively and efficiently review potential security vulnerabilities or issues and allowing for quicker remediation if required.

Procedures for investigating unauthorized activity vary according to the type and scope of event. At a minimum, NCO policy mandates we perform the following steps:

- Notify the incident response team and activate incident response plan.
- Immediately initiate manual backup procedures on systems under suspicion.
- Identify approximate time period of suspected unauthorized activity.
- Identify true scope of intrusion and damage, involving NCO legal team, relevant customers (via business relationship manager), partners, and law enforcement as necessary.
- Generate ad-hoc reports from intrusion detection and host systems filtered to that timeframe.
- Correlate events from systems reports to identify suspicious activity.
- Disable any accounts used for unauthorized access or activity.
- Notify credit card associations and acquirers if applicable.

System Security

ID/Password
NCO policy defines standards for password creation, protection, and frequency of change. Our centralized IT help desk maintains responsibility for user credential creation, changes, and deletions for our mission critical applications. In addition to business unit management approval, IT management must approve additions and/or changes for accounts having higher levels of privilege than a standard agent representative. Session inactivity time-out policies and procedures are implemented across our systems to automatically log users off after a specified period of time at both the application and workstation levels.

Virus Protection
NCO mitigates threats from viruses by deploying multi-tiered, enterprise-wide anti-virus solutions which encompass the workstation, server and infrastructure components.

Security Standards
Operational and security benchmarks are reviewed and recorded upon an initial server build while regular scans are conducted on a weekly, monthly, and quarterly basis to ensure compliance with approved standards and processes. Testing processes and procedures are re-evaluated and updated as needed.

Security Testing
NCO performs internal vulnerability testing and scans on a periodic basis. This testing is augmented with unannounced third-party testing, on a yearly basis, to accurately determine and mitigate potential threats and risks. As critical vulnerabilities are discovered, potential impacts/threats/risks are evaluated and remediation is scheduled – if applicable or compensating controls do not exist. These processes and procedures are key in validating our information security performance and assessing how well we are protecting the integrity and confidentiality of client data.

Third-Party Security Assessments

NCO's technology data center has undergone numerous security reviews, risk assessments, and safety and soundness checks. Many of our larger financial customers conduct scheduled risk reviews of our corporate headquarters and remote call centers.

Below is a list of completed assessments:

- SAS 70, Type II
- Payment Card Industry (PCI), Level 1 Service Provider certification has been satisfied by a third-party onsite review (formerly VISA Cardholder Information Security Program, MasterCard SDP, and American Express DSS)
- Quarterly, third-party vulnerability scans/assessments

Personnel

All NCO employees are expected to perform their daily responsibilities in an honest, ethical, and professional manner. NCO employees:

- Must comply with all applicable federal, state, local and international laws and regulations at all business locations and operations
- Are required to maintain the privacy and confidentiality of sensitive personal data placed in our trust by a client, including data in our possession that we may have access to, and an individual's financial, medical, or employment data
- May not communicate proprietary or confidential NCO information to competitors, including client data, corporate pricing policy, or marketing and systems plans
- May not use or share "inside information" that is not generally available to the general public for any manner of direct or indirect personal gain or other unauthorized use
- Must comply with all applicable employment requirements for lawful employment

Information Protection Oversight

NCO has a designated corporate compliance officer who ensures we comply with all applicable laws and regulations affecting our industry. We also have a Vice President of Information Security responsible for overseeing the implementation of security projects, audits, and testing, and ensuring our formal incident response is effective and appropriate. Our Senior Vice President of Corporate Security is responsible for monitoring fraudulent activity and physical security of NCO facilities.

Certifications

NCO highly values the opportunity to appropriately mentor and facilitate professional certifications for its personnel. Our IT department has a total of six CISSP certified technicians, one re-certified CCIE, one Enterasys Security Certified technician, one Cisco Pix Firewall, one Checkpoint Firewall experienced technician, one CCNE, and five CCNP certified technicians.

Employee Background Checks

NCO conducts background checks for felony records, previous employment, education, and personal references for new hires. We tailor our hiring standards to each client program, and we will conduct any background investigation required to support said programs, including comprehensive background checks, credit investigations, fingerprinting, bonding, or drug testing.

Awareness and Education

Security awareness and education are incorporated into the orientation and training of new employees. Employees must review and acknowledge the receipt of the Employee Handbook, which includes NCO's Acceptable and Unacceptable Use policy. This policy explains NCO's security requirements and relative privacy regulations. Additionally, agents are required to renew their acknowledgement of the Information Security policy on a yearly basis depending upon client requirements.

Clean Desk Policy

Due to the extremely sensitive nature of the information we manage, NCO's employees operate in a "clean desk" environment. Employees are instructed to maintain a clean desk prior to leaving any work area. While the information protected by this measure includes documents classified as 'Confidential Customer', 'Confidential Corporate,' and 'Internal Use' other sensitive information specific to various departments may also apply. This type of information must be visibly removed from the work area and locked in a secure device or cabinetry prior to leaving the work area.

All employees must:

- Remove all hardcopy documents with sensitive information from their work area prior to leaving their work area
- Remove all hard copy sensitive documents from printers immediately upon sending it to print
- Ensure all unclaimed sensitive hardcopies left in print areas are shredded at the end of the day
- Clean all whiteboards after use
- Ensure message/cork boards are free of sensitive information
- Lock their computers before leaving their work area
- Ensure sensitive display areas are out of view in high traffic areas (e.g., the use of screen protectors and blinds is encouraged)
- Password-protect PDAs, organizers, company-issued phones and laptops
- Not leave passkeys, ID badges, or keys unprotected; must lockup or keep with them
- Lock all sensitive material in cabinets
- Remove all USB "thumb" drives, floppy disks, CDs, DVDs, or other data media containing any sensitive or confidential information from their work area prior to leaving their work area

Compliance

NCO conducts its business in strict compliance with all applicable U.S. and international laws and regulations governing business conduct, including information protection, security transactions, environmental protection, and employment.

- NCO complies with the Electronic Fund Transfer Act as it applies to our services.
- NCO complies with the Fair Credit Reporting Act (FCRA), which regulates the privacy and accuracy of information provided by the consumer credit reporting industry. The FCRA and the FDCPA are administered and enforced by the Federal Trade Commission (FTC).
- NCO complies with the provisions of the Gramm-Leach-Bliley Act as they affect our outsourcing relationships, relative to the sharing of nonpublic, personal financial information.
- NCO complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which establishes privacy standards and procedures for handling patient and health information relative to collecting healthcare receivables.
- NCO understands and complies with the Family Educational Rights and Privacy Act (FERPA), 34 CFR Part 99, regarding the protection and privacy of student education records as it applies to our services.

Reporting Suspicious Activity

By using call monitoring procedures, management observation, and review of transaction trends, along with our stringent physical environment and data security measures, NCO adheres to rigorous suspicious activity reporting requirements.

Suspicious activity(ies) witnessed by and/or reported to management results in the following escalation chain:

Addressing Suspicious Activity	
Immediate notification	▪ Site Quality Department ▪ Site Operations / Shift manager ▪ Site General Manager
Resource Notification	▪ Corporate Director of Operations ▪ Corporate Security Manager ▪ Corporate Senior VP of Operations ▪ Corporate Employee Relations Manager ▪ Client Contacts as required

At time of such activity, the suspected individual(s) is immediately removed from calling activities and/or suspended from active duty to allow time for an investigation to be completed.

Investigations are documented using standard HR procedures relating to employee behavior and fraud. In addition, NCO is willing to adopt and conform to procedures related to these matters as prescribed by our clients.

Compliance Hotline

Every NCO employee has the responsibility to report any real or suspected violation of the NCO's Standards of Conduct. To provide complete confidentiality in reporting any violation of the law or fraudulent activity, NCO has established a Compliance Hotline. The purpose of the Compliance Hotline is to provide NCO employees a 24-hour, third-party hotline monitoring and reporting service to assist in addressing possible unethical, illegal, or questionable behavior that cannot be resolved at the local facility. Calls to the Compliance Hotline are completely confidential and may be made anonymously if preferred.

Findings of NCO policy violations, criminal or illegal conduct may result in disciplinary action up to and including immediate termination, as well as referral to law enforcement agencies.

Insurance and Bonding

NCO carries liability insurance to protect its interests and the interests of its clients. Coverage is in place for major categories including:

Category	Amount
General liability	$2,000,000
Automobile liability	$1,000,000
Excess liability	$25,000,000
Workers compensation & employers liability	$500,000
Errors and omissions	$25,000,000

Additionally, all NCO employees are bonded in the amount of $20 million per occurrence for employee dishonesty, depositor's forgery, computer fraud, and money loss.

Note: NCO provides coverage for Technology Errors and Omissions/Internet Liability and Network Security Liability under our existing insurance policy. If a client requires a separate rider for this coverage, we are happy to comply.