NCID Security Policies

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. North Carolina Information Data, Inc. (NCID) understands the critical nature of protecting your data and has prepared this document to help you understand the security measures and policies we have in place.

NCID servers are located in a SSAE 16 certified data center by Windstream Hosted Solutions. Windstream's comprehensive portfolio of data protection services including rigorous physical security checks, redundant connections to the Internet backbone, state-of-the-art firewalls, redundant backup power supplies, managed monitoring of servers and managed backup services. Web Application Firewalls protect our sites against Distributed Denial of Service attacks and other "hacker" threats.

Threats

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence to its customers.

The CIA triad of **confidentiality**, **integrity**, and **availability** is at the heart of information security. We preserve the confidentiality of your data through many layers of security where it is only accessible by authorized persons. Data integrity is rigorously maintained by expert engineers through accurate analysis and reporting. Information availability is the hallmark of NCID, where you can easily and promptly get the accurate information you need.

Access Control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. Access control is generally considered in three steps: Identification, Authentication, and Authorization.

Identification

is an assertion of who someone is or what something is. Typically the claim is in the form of a username. The identification of everyone requesting access to any secured data is checked against our databases of authorized users. Physical access to servers is restricted by the Windstream data center.

Authentication

is the act of verifying a claim of identity. By entering the correct password, the user is providing evidence that they are the person the username belongs to for online access. For physical access driver's license or other State ID must match the authorized access list.

Authorization

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization.

NCID customers may subscribe to different products and thus are only authorized to use those products. Our software is designed to determine which users can access certain products. The software also separates users of common products, so no one else can ever access your private data. At the employee level, NCID personnel are only authorized to access data that they need to directly work with.

Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used by NCID to store sensitive data such as credit card numbers.

Data Transmission

Data transmitted over the Internet is susceptible to several types of abuse, from intentional interception (sniffing) to interruptions in Internet service. NCID uses encryption for the transmission of all sensitive data. Our websites are protected by powerful SSL certificates using SHA-2 and 2048-bit encryption. All email from NCID personnel are also encrypted. All external access to our servers from outside engineers is through IPsec encrypted Virtual Private Networks.

NCID is constantly striving to update and improve our security measures and policies. To this end, this document may not be 100% accurate at any given point in time. But please be assured any changes we make are done with your data integrity as the foremost goal.

Call 800.792.4339 with any questions.