



## ACCESS SECURITY REQUIREMENTS

It is a requirement that all end users take precautions to secure any system or device used to access consumer credit information. To that end, the following requirements have been established:

### 1. Implement Strong Access Control Measures

- 1.1 Your account number and password must be protected in such a way that this sensitive information is known only to key personnel. Under no circumstances should unauthorized persons have knowledge of your password. The information should not be posted in any manner within your facility. Do not provide account numbers, Subscriber Codes or passwords to anyone.
- 1.2 Any system access software you may use, whether developed by your company or purchased from a third party vendor, must have your account number and password "hidden" or embedded so that the password is known only to supervisory personnel.
- 1.3 Each user of your system access software must then be assigned unique log-on passwords. Develop strong passwords that are:
  - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
  - obtain a minimum of seven (7) alpha/numeric characters for standard user accounts
  - Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
  - Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.4 You must request your account number, Subscriber Code and/or password be changed immediately when:
  - Any system access software is replaced by another system access software or is no longer used;
  - The hardware on which the software resides is upgraded, changed or disposed of.
- 1.5 Your account number and passwords are not to be discussed by telephone to any unknown caller, even if the caller claims to be an employee.
- 1.6 Create a separate, unique user ID's for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.7 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.8 The ability to obtain credit information must be restricted to a few key personnel.
- 1.9 Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
- 1.10 Implement a process to terminate access rights immediately for users who access credit reporting agency credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
- 1.11 Any terminal devices used to obtain credit information should be placed in a secure location within your facility. Access to the devices should be difficult for unauthorized persons.
- 1.12 Any devices/systems used to obtain consumer reports should be turned off and locked after normal business hours, when unattended by your key personnel.
- 1.13 Consumer reports containing personally identifiable information should not be downloaded onto a laptop computer or other mobile device.



- 1.14 Hard copies and electronic files of consumer reports are to be secured within your facility and protected against release or disclosure to unauthorized persons.
- 1.15 Hard copy consumer reports are to be shredded or destroyed, rendered unreadable, when no longer needed and when it is permitted to do so by applicable regulations(s).
- 1.16 Electronic files containing consumer report data and/or information will be completely erased or rendered unreadable when no longer needed and when destruction is permitted by applicable regulation(s).
- 1.17 Software cannot be copied. Software is issued explicitly to you solely to access reports for permissible purposes.
- 1.18 Your employees will be forbidden to attempt to obtain credit reports on themselves, associates or any other persons, except in the exercise of their official duties.

## **2. Maintain a Vulnerability Management Program**

- 2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- 2.2 Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
- 2.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
  - Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
  - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
  - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
  - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
  - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
  - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
  - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

## **3. Protect Data**

- 3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)
- 3.2 All credit reporting agency data is classified as Confidential and must be secured to this requirement at a minimum.



- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

#### **4. Maintain an Information Security Policy**

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

#### **5. Build and Maintain a Secure Network**

- 5.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- 5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- 5.4 Any stand alone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.
- 5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

#### **6. Regularly Monitor and Test Networks**

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:
  - protecting against intrusions;
  - securing the computer systems and network devices;
  - protecting against intrusions of operating systems or software