

ACCESS SECURITY REQUIREMENTS

In accessing Intelius Screening Reports, Company agrees to follow these security requirements:

1. Implement Strong Access Control Measures

- a) Account access credentials and passwords should not be shared. Intelius representatives will never request your password.
- b) Request passwords are changed immediately when the hardware from which Screening Reports are accessed is upgraded, changed or disposed of.
- c) Create a separate, unique user ID for each user to enable individual authentication and accountability for access to Intelius Screening Reports.
- d) Ensure that no Peer-to-Peer file sharing is enabled.
- e) Develop strong passwords that are not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- f) Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- g) Restrict the number of key personnel who have access to Screening Reports.
- h) Ensure that personnel who are authorized access to Screening Report information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose section of your membership application.
- i) Ensure that employees do not access their own Screening 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.
- j) Implement a process to terminate access rights immediately for users who access Intelius Screening reports when those users are terminated or when they have a change in their job tasks and no longer require access to that information.
- k) After normal business hours, turn off and lock all devices or systems used to obtain Screening Reports.
- l) Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain Screening Reports.

2. Maintain a Vulnerability Management Program

- a) Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- b) 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.
- c) Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
 - a. Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
 - b. 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.

- c. 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.
- d. Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
- e. Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
- f. 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.
- g. Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
- h. 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

- a) 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.)
- b) Treat all Intelius Screening Report data as Confidential and be sure it is secured to this requirement at a minimum.
- c) Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- d) Encrypt all Intelius 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.
- e) Only open email attachments and links from trusted sources and after verifying legitimacy.

4. Maintain an Information Security Policy

- a) Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- b) 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.
- c) 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.
- d) 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

- a) Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
 - a. Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet.
 - b. Network address translation (NAT) technology should be used.
- b) Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- c) 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.
- d) Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- e) 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

- a) Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- b) 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 Intelius 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:
 - a. protecting against intrusions;
 - b. securing the computer systems and network devices;
 - c. and protecting against intrusions of operating systems or software.