Access Security Requirements

Last Modified: January 9, 2015

The following information security controls are required to reduce unauthorized access to consumer information. It is Subscriber's responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. ID reserves the right to make changes to these Access Security Requirements without prior notification. The information below provides minimum baselines for information security. In accessing the Services, Subscriber agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store the Services and/or Information:

1. Implement Strong Access Control Measures

1.1.1 All credentials such as user names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from ID will ever contact you and request your credentials.
1.2 If using third party or proprietary systems to access Services, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing ID Services.
1.3 If the third party or third party software or proprietary system or software, used to access ID Services, is replaced or no longer in use, the passwords should be changed immediately.
1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to ID's infrastructure. Each user of the system access software must also have a unique logon password.
1.5 User IDs (defined below) and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.
1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.
1.7 Develop strong passwords that are:
• Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers/letters)
• Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
• For interactive sessions (i.e. non system-to-system) ensure that passwords are changed periodically (every 90 days is recommended)
1.8 Passwords must 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
• Any suspicion of password(s) being disclosed to an unauthorized party (see section 4.3 for reporting requirements)
1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithms are utilized (e.g. AES 256 or above).
1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.
1.11 Active logins to ID systems must be configured with a 30 minute inactive session timeout.
1.12 Ensure that personnel who are authorized access to Services have a business need to access such Services and understand these requirements to access such Services are only for the permissible uses listed in the GLBA Permissible Use section of the Subscriber Agreement.
1.13 Subscriber must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Services and/or Information.
1.14 Ensure that Subscriber employees do not access their own Information or those reports of any family member(s) or friend(s) unless it is in connection with a permissible use.
1.15 Implement a process to terminate access rights immediately for users who access the Services when those users are terminated or when they have a change in their job tasks and no longer require access to the Services.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.
1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.
1.18 Implement physical security controls to prevent unauthorized entry to Subscriber's facility and access to systems used to obtain the Services. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.
2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and 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 anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
• Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
• If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

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 ID's Information is classified confidential and must be secured in accordance with the requirements mentioned in this document 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 ID's Information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.
3.5 ID's Information must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.
3.6 When using smart tablets or smart phones to access ID's Services, ensure that such devices are protected via device passcode.
3.7 Applications utilized to access ID's Services via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.
3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.
3.9 When no longer in use, ensure that hard-copy materials containing Information are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
3.10 When no longer in use, electronic media containing Information is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

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 Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.
4.3 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.
4.4 Implement appropriate measures to dispose of any Information that will protect against unauthorized access or use of that Information.
4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the 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 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.
5.6 For wireless networks connected to or used for accessing or transmission of ID's Services/Information, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.
5.7 When using service providers (e.g. software providers) to access Services, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)
6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Services/Information; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.
6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to access Services. 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 (including operating systems and software); and
• securing the computer systems and network devices.

7. Mobile and Cloud Technology

7.1 Storing Information on mobile devices is prohibited.
7.2 When using cloud providers to access, transmit, store, or process Services/Information, ensure that:
• Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations.
• Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Interactive Data:
• ISO 27001
• PCI DSS
• EI3PA
• SSAE 16 – SOC 2 or SOC3

• FISMA
• CAI / CCM assessment

8. General

8.1 ID may from time to time audit the security mechanisms Subscriber maintains to safeguard access to Services/Information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices.
8.2 In cases where the Subscriber is accessing Services/Information via third party software, Subscriber agrees to make available to ID upon request, audit trail information and management reports generated by the vendor software, regarding Subscriber Authorized Users (defined below).
8.3 Subscriber shall be responsible for and ensure that third party software, which accesses Services, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.
8.4 Subscriber shall conduct software development (for software which accesses Services; this applies to both in-house or outsourced software development) based on the following requirements:
8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.
8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.
8.5 Reasonable access to audit trail reports of systems utilized to access Services shall be made available to ID upon request, for example during breach investigation or while performing audits.
8.6 Services requests from Subscriber to ID must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.
8.7 Subscriber shall report actual security violations or incidents that impact ID to ID within twenty-four (24) hours or per agreed contractual notification timeline. Subscriber agrees to provide notice to ID of any confirmed security breach that may involve Services/Information, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 678-584-5252; Email notification will be sent to Incident@id-info.com.
8.8 Subscriber acknowledges and agrees that Subscriber (a) has received a copy of these requirements, (b) has read and understands Subscriber's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Services/Information, and (d) will abide by the provisions of these requirements when accessing Services/Information.
8.9 Subscriber understands that its use of ID networking and computing resources may be monitored and audited by ID, without further notice.
8.10 Subscriber acknowledges and agrees that it is responsible for all activities of its Authorized Users, and for assuring that mechanisms to access Services/Information are secure and in compliance with its Subscriber Agreement.
8.11 When using third party service providers to access, transmit, or store Services/Information, additional documentation may be required by ID.

Internet Delivery Security Requirements

In addition to the above, the following requirements apply where Subscriber is provided access to Services via the Internet ("Internet Access").

General requirements

1. Subscriber shall designate in writing, an employee to be its Head Security Designate (defined below), to act as the primary interface with ID on systems access related matters. The Subscriber's Head Security Designate will be responsible for establishing,

administering and monitoring all Subscriber employees' Internet Access, or approving and establishing Security Designates to perform such functions.
2. Subscriber's Head Security Designate or Security Designate shall in turn review all employee requests for Internet Access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each of the Services based upon the legitimate business needs of each employee. ID shall reserve the right to terminate any accounts it deems a security threat to its Services, systems and/or Information.
3. Unless automated means become available, Subscriber shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by ID. Those employees approved by the Head Security Designate or Security Designate for Internet Access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). ID's approval of requests for Internet Access may be granted or withheld in its sole discretion. ID may add to or change its requirements for granting Internet Access at any time (including, without limitation, the imposition of fees relating to Internet Access upon reasonable notice to Subscriber), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. Note: Partially completed forms and verbal requests will not be accepted.
4. An officer of Subscriber agrees to notify ID in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Subscriber agrees to identify an employee it has designated to act on its behalf as a primary interface with ID on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Subscriber and shall be available to interact with ID on information and product access, in accordance with these Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of Subscriber. Subscriber's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Subscriber's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to ID's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to ID immediately.
2. As a subscriber to Services via the Internet, the Head Security Designate is acting as the duly authorized representative of Subscriber.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Subscriber authorizes to act on behalf of the business in regards to ID Services access control (e.g. request to add/change/remove access). The Subscriber can opt to appoint more than one Security Designate (e.g. for backup purposes). The Subscriber understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with ID's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding ID representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to Services) that are required to be terminated due to suspicion of (or actual) threat of system compromise, unauthorized access to Services and/or Information, or account inactivity.

Designate

1. Is responsible for the initial and on-going authentication and validation of Subscriber's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
2. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
3. Is responsible for ensuring that Subscriber's Authorized Users are authorized to access Services.
4. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Subscriber.

5. Must immediately report any suspicious or questionable activity to ID regarding access to ID's Services/Information.
6. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to ID.
7. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
8. Shall be available to interact with ID when needed on any system or user related matters.