Access Security Requirements

Last Modified: July 26, 2023

The security requirements included in this document ("Access Security Requirements") represent the minimum, acceptable security requirements and are intended to ensure that a Subscriber has appropriate controls in place to protect information and systems, including any Services containing information that is collected, processed, sold or disclosed pursuant to the GLBA and/or DPPA that Subscriber receives, processes, transfers, transmits, stores, delivers, and/or otherwise accesses.

DEFINITIONS

"Information" means highly sensitive information including, by way of example and not limitation, data, databases, application software, software documentation, supporting process documents, operation process and procedures documentation, test plans, test cases, test scenarios, cyber incident reports, consumer information, financial records, employee records, and information about potential acquisitions, and such other information that is similar in nature or as mutually agreed in writing, the disclosure, alteration or destruction of which would cause serious damage to ID's or ID's third-party sources' reputation, valuation, and / or provide a competitive disadvantage to ID or ID's third-party sources.

"Resource" means all Subscriber devices, including but not limited to laptops, PCs, routers, servers, and other computer systems that store, process, transfer, transmit, deliver, or otherwise access Information.

1. Information Security Policies and Governance

Subscriber shall have information security policies and procedures in place that are consistent with the practices described in a comprehensive, industry-standard information security standard, such as ISO 27002. Subscriber's policies and procedures must also comply with these Access Security Requirements. In the event of any conflict between these Access Security Requirements and any other terms and conditions agreed to by the parties, the terms that impose the greatest protection to Information shall apply.

2. Vulnerability Management

Firewalls, routers, servers, PCs, and all other resources managed by Subscriber (including physical, on-premises, or cloud hosted infrastructure) will be kept current with appropriate security specific system patches. Subscriber will perform regular penetration tests to further assess the security of systems and resources. Subscriber will use end-point computer malware detection / scanning services and procedures.

3. Logging and Monitoring

Logging mechanisms will be in place sufficient to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted, or locked) with a process for periodic review.

4. Network Security

Subscriber will use security measures, including anti-virus software that is updated regularly, to protect communications systems and networks device to reduce the risk of infiltration, hacking, access penetration by, or exposure to, an unauthorized third-party.

5. Data Security

Subscriber will use security measures, including but not limited to 128 bit or higher encryption, to protect Information in storage and in transit to reduce the risk of exposure to unauthorized parties.

6. Remote Access Connection Authorization

All remote access connections to Subscriber internal networks and / or computer systems will require authorization with access control at the point of entry using multi-factor authentication. Such access will use secure channels, such as a Virtual Private Network (VPN).

7. Incident Response

Processes and procedures will be established for responding to security violations and unusual or suspicious events and incidents. Subscriber will report actual or suspected security violations or incidents that may affect ID or ID's third-party sources to ID within twenty-four (24) hours of Subscriber's confirmation of such violation or incident.

8. Identification, Authentication and Authorization

Prior to granting any user access to the Services, Subscriber shall conduct or cause to be conducted background screening of each user that is consistent with applicable laws and reasonable in relation to Subscriber's size and complexity, the nature and scope of its activities, and the sensitivity of the Information provided to Subscriber by ID. Subscriber shall retain documentation establishing the completion of appropriate background screening.

Each user of any Resource will have a uniquely assigned user identification to enable individual authentication and accountability. Access to privileged accounts will be restricted to those people who administer the Resource and individual accountability will be maintained. All default passwords (such as those from hardware or software vendors) will be changed immediately upon receipt.

9. User Passwords and Accounts

All passwords will remain confidential and use 'strong' passwords that expire after a maximum of 90 calendar days. Accounts will automatically lockout after five (5) consecutive failed login attempts.

10. Training and Awareness

Subscriber shall require all Subscriber personnel to participate in information security training and awareness sessions at least annually and establish proof of learning for all personnel.

11. ID's Right to Audit

Subscriber shall be subject to remote and / or onsite assessments of its information security controls and compliance with these Access Security Requirements.

12. Bulk Email Communications into ID

Subscriber will not "bulk email" communications to multiple ID employees without the prior written approval of ID. Subscriber shall seek authorization via their ID account representative in advance of any such campaign.