

Security Guidelines

It is imperative that all Designates and End Users fully understand and adhere to our comprehensive security guidelines.

General

1. Experian fully recognizes its obligations to support and implement practices, which protect the confidential nature of the information in our databases and assure respect for consumers' right to privacy. Therefore, only companies that are approved members of our services ("Clients") and have permissible purpose for obtaining credit and other reports are permitted to access the applications that Experian provides to access this sensitive data.
2. To this end, it is important that all Clients take appropriate precautions to secure any systems (hardware and software) used to access Experian's information systems and ensure that all of the Client's personnel who have been granted access to Experian's information systems adhere to the security guidelines provided herein.
3. These guidelines describe the general expectations and security requirements with respect to handling information, access to, and usage of Experian's information systems by its Clients, Affiliates and End Users. One of the purposes of these guidelines is to clarify the standards of behavior required of Clients and persons who have been granted access to Experian's information system assets. It is the responsibility of each system user to ensure that all possible measures are used to protect the confidential nature of the information that is handled and to protect the integrity of the systems providing this information.
4. As security threats and vulnerabilities, along with the technologies and methods available to mitigate the resultant risks is an ever-changing landscape, these guidelines may periodically change to reflect this new environment.

Guidelines

1. A Client shall obtain users' (Internet) access to Experian's services only through the individual Client employees who Client's Head Designate specifically approves and submits to Experian for approval and setup (each an "Authorized Employee"). Client shall request (Internet) access in writing in a format approved by Experian. Authorized Employees will be assigned unique access identification numbers ("User ID") and passwords (this also applies to the unique server-to-server access IDs and passwords). Experian's approval of requests for (Internet) access may be granted or withheld at its sole discretion. Experian may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Client), and reserves the right to change passwords and to revoke any authorizations previously granted.
2. Only Authorized Employees shall access Experian's services (via the Internet) and only through the User ID and password assigned to such employee by Experian or by the security Head Designate (as delegated and approved by Experian). Clients shall request User IDs and passwords only for those employees of customer who have a legitimate need to access the services in performing his or her duties for the client. Prior to requesting and assigning User IDs for Authorized Employees, Client shall provide adequate training regarding these procedures and any applicable laws. Client will ensure that each Authorized Employee (i) is familiar with the requirements specified herein and agrees to comply with such requirements, (ii) agrees not to disclose the User ID and password assigned to the Authorized Employees to any other person and (iii) agrees not to order credit reports or other data from Experian except in performance of employee's official duties for Client.
3. Client acknowledges and agrees that it is responsible for all activities of its employees in utilizing the Internet to access Experian's services and for assuring the facilities for receipt of information provided to it through the Internet are secure and in compliance with Client's membership or customer agreement(s) covering such services. Client shall not retransmit or otherwise make available to any person the services

(including any of the information therein) on or through the Internet or other generally accessible network or delivery method.

4. Client acknowledges and agrees that these guidelines and procedures are in addition to the procedures of the membership application process including any access security requirements (except where expressly modified by these Experian security guidelines). Client will abide by any additional or further security procedures specified by Experian from time to time.
5. Client shall use its best efforts to ensure the confidentiality of all User IDs and passwords issued. Client shall indemnify Experian against any damage or disruption to Experian's systems or business caused by customer's employees, subcontractors, subcontractor employees or its clients whether as a result of their access to such systems or compromise of password confidentiality or otherwise.
6. Client understands that its use of Experian networking and computing resources may be monitored and audited by Experian without further notice. Experian may from time to time audit the security mechanisms customer maintains to safeguard access to Experian's information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices.
7. In cases where the Client is accessing Experian's information and systems via Experian's certified software, the Client agrees to have available upon request, audit trail information and management reports regarding the Client's individual users.
8. Client shall be responsible for and agrees to provide a standard of care to ensure that Experian's certified vendor software, which accesses Experian's information systems, is secure and protects against unauthorized modification, copy and placement on systems which have not been authorized for its use.

Reporting

1. An officer of Client's company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Designate, Security Designate or End User; or if the identified Head Designate, Security Designate or End User is terminated or otherwise loses his or her status as an Authorized Employee.
2. Audit trail reports shall be made available to Experian upon request.
3. Client agrees to report to Experian's Information Security Office any compromise or suspected compromise of security which may lead to a compromise or threat to Experian's information systems.

Roles and responsibilities

Head Designate

1. Client agrees to identify an individual it has designated to act on their behalf as a primary interface with Experian on (Internet) access related issues. This individual shall be identified as the "Head Designate." The Head Designate will submit all requests to create, change or lock Designate and/or End User access accounts and permissions to Experian's systems and information (via the Internet). Designate(s) must be an authorized representative of the Client's company and must be available to interact with Experian on information and product access in accordance with [Experian's security guidelines](#). The (Head) Designate authorization forms must not be accepted unless signed by an authorized representative of the Client. Changes in (Head) Designate status (e.g., transfer or termination) are to be reported to Experian immediately.
2. As a Client to Experian's products and services over the Internet, the Head Designate is acting as the authorized representative of the Client.
3. The Head Designate is the individual that Client authorizes to act on behalf of the business in regards to Experian's product access control (e.g., request to add/change/remove (Internet) access). Client can opt to appoint more than one designate (e.g., for backup purposes). Client understands that the Designate(s) it appoints must be someone who will be available between the hours of 8:00 a.m. to 5:00 p.m. (normal business hours) and can liaison with Experian on information and product access matters.

Designate

1. Must be an authorized representative of Client's company, identified as a single approval point for Client's users.
2. Is responsible for the initial and on-going authentication of Client's users and must maintain current information about each (phone number, valid email address, etc.).
3. Must notify Experian, if no automated facilities are provided, to add, change, and lock users within Client's company.
4. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized Employee's job responsibilities.
5. Must ensure that standard security administration functions are performed within Client's company. These include periodic review of Authorized Employee's activities, Authorized Employee's access rights, inactivity reviews, authentication and authorization process review, etc.
6. Is responsible for ensuring that Client's users are authorized to access Experian's products and services.
7. Must disable User ID if it becomes compromised or if the Authorized Employee's employment is terminated by Client.
8. Ensure password and ID records remain secure in Client's customer environment.
9. Must advise users not to share/post password or ID information.
10. Must advise users of their responsibility to access consumer information for specified business uses only.
11. Must advise users not to leave their workstations unattended when accessing Experian products and services.
12. Must advise users to secure any Experian provided or generated documentation.
13. Must immediately report any suspicious/questionable activity to Experian regarding Experian's product access to Experian's products and services.
14. Must report any potential compromise of Client's systems that may expose Experian provided products or data to security threats.
15. Must communicate to users the security practices and regularly audit same within Client's organization.
16. Must immediately report changes in Head Security Designate status (e.g. transfer or termination) to Experian. Client's authorized representative must authorize changes to Client Head Designate.
17. You will be informed of any inquiries about passwords or IDs requested of Experian by your Users. Experian reserves the right to audit the processes employed and the documentation used to ensure Client's User ID and password security. Any weakness or lack of documentation as well as any User ID or password compromise may result in termination of Client's access rights.
18. Must be available to interact with Experian when needed on matters of user access and authorization.

Users

1. Shall use only the User ID and password which has been assigned to them. These User IDs and passwords are not to be shared and each user shall be held accountable for all actions which occur under that User ID.
2. Shall immediately notify the Security Designate or Head Designate when the information resource access is no longer required.
3. Shall protect their assigned User ID and password from unauthorized use.

Dos and don'ts

User IDs and passwords

The following are just a few guidelines that should be considered by users in constructing passwords:

1. Do **not** use your login name in any form (i.e., as is, reversed, caps, doubled, etc.).
2. Do **not** use your first, middle or last name in any form.

3. Do **not** use other information easily obtained about you (i.e., employee number, child or spouse's name, address., etc.).
4. Do **not** use a password of all digits, or all the same letters.
5. Do **not** use a word contained in English or foreign language dictionaries.
6. Do **not** use a password shorter than six characters.
7. **Do** use a password with mixed case alphabetic.
8. **Do** use a password that is easy to remember so you don't have to write down.
9. **Do** change your password often enough to prevent an unauthorized person from guessing your password (every 90 days is suggested).
10. **Do** change your password **immediately** if you believe it has been compromised and notify the Security Administrator.
11. **Do** change your password the first time you log onto a new system.

Other general guidelines to follow include:

1. Do **not** share your password with anyone. (even Security Administrators should not be asking you for your password).
2. Do **not** share your user account or allow anyone to use your account while your workstation is unattended (log off or the use of password controlled screen savers can help reduce this risk).
3. Do **not** write your password down and post it (or try to hide it) in an obvious location (i.e., don't post-it on your monitor, hide it in your desk calendar, under your desk pad or keyboard, etc.).
4. Do **not** repeat your passwords for at least 18 iterations.
5. **Do** notify the Security Administrator when the account is no longer needed.