zeroedin
people analytics

Complementary User Entity Controls

ZeroedIn's services are designed with the assumption that user entities will implement certain security controls. Such controls are called complementary user entity controls. It is not feasible to achieve 100% security risk mitigation related to ZeroedIn's services solely through ZeroedIn implemented security control procedures. Accordingly, user entities in conjunction with the services, should establish their own internal controls or procedures to complement those of ZeroedIn.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the highest level of risk mitigation is achieved. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities security auditors should exercise judgement in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to ZeroedIn.
2. User entities are responsible for notifying ZeroedIn of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management, and control of the use of ZeroedIn services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ZeroedIn services.
5. User entities should implement Single Sign-On (SSO) using a trusted Identify Provider for user authentication when possible.
6. User entities are responsible for restricting access to security and account management privileges within ZeroedIn to appropriate personnel only.
7. User entities are responsible for implementing least privilege when assigning security access to ZeroedIn users.
8. User entities are responsible for ensuring that user accounts and passwords to ZeroedIn are not shared.
9. User entities are responsible for ensuring that users who no longer require access to ZeroedIn have their privileges revoked in a timely manner.
10. User entities are responsible for reviewing existing user accounts and security role grants on a regular basis to determine if user account access and/or privileges are still needed.
11. User entities are responsible for immediately notifying ZeroedIn of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
12. User entities are responsible for ensuring that users receive initial and refresher training on Security Awareness.
13. User entities are responsible for ensuring that users receive initial and refresher training on Identifying and Safeguarding Personally Identifiable Information (PII).

14. User entities are responsible for minimizing transmission of sensitive and personally identifiable information such as social security numbers and date of birth.
15. User entities are responsible for ensuring that secure encryption methods are utilized when transporting data to ZeroedIn.
16. User entities are responsible for minimizing data export requests to include only the necessary data fields required to support the data export use case.
17. User entities are responsible for minimizing the sending and transfer of PII or other sensitive data when creating support tickets in ZeroedIn's Support System.

Last revised: February 6, 2024