cenareo

Cyber Security - Access Management

This policy ensures that access to sensitive information and systems is granted based on the principle of least privilege and helps to mitigate the risk of unauthorized access.

Identity and Access Management (IAM)

Cenareo maintains documented processes for Identity and Access Management (IAM) for both internal and external users.

The IAM program is subject to regular review and updates to reflect changes in technology, industry best practices, and regulatory requirements.

These processes cover the entire user lifecycle, including:

- **Joiners**: New employee accounts are created with appropriate access rights based on their job role and responsibilities.
- **Movers**: When an employee's role or department changes, their access rights are reviewed and adjusted accordingly.
- **Terminations**: Upon termination of employment, all user accounts and access privileges are promptly disabled or deleted.
- **External Users**: Access for external users (contractors, vendors, etc.) is granted based on the principle of least privilege and the specific needs of their role.

Access Recertification

Access rights for all users (internal and external) are reviewed and recertified periodically to ensure continued need and adherence to the principle of least privilege.

Role-Based Access Control (RBAC)

We implement Role-Based Access Control (RBAC) as the primary method for managing user access to systems and applications. Under RBAC:

- **Roles**: Predefined roles are established, each with a specific set of permissions and access rights aligned with typical job functions and responsibilities.

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

- **User Assignment**: Users are assigned roles based on their job requirements.
- **Least Privilege**: Users are granted the minimum set of privileges necessary to perform their assigned duties effectively.

User Access Review Frequency

- **Business Users**: User access rights for business users are reviewed at least annually or upon a significant change in role or responsibilities.
- **Privileged Users**: Access rights for privileged users (e.g., system administrators) are reviewed quarterly due to the higher risk associated with their elevated permissions.
- **Generic/Shared Accounts and System/Service Accounts**: Access rights for generic/shared accounts and system/service accounts are reviewed semi-annually to ensure they are still necessary and used appropriately.

Unauthorized Access Detection

We have implemented controls to detect unauthorized access attempts. These controls include:

- **User Activity Monitoring**: User activity on critical systems is monitored for suspicious behavior.
- **Log Management**: System logs are collected and analyzed for unauthorized access attempts.
- **Access Reviews**: Regular access reviews help identify discrepancies and potential misuse of access privileges.
- **Strong Password Policies**: Enforcing strong password policies and multi-factor authentication helps prevent unauthorized access.

Privileged Access Management

In addition to the access review processes outlined above, we implement additional controls for privileged access management including:

- **Just-In-Time (JIT) Privileged Access**: Granting elevated privileges only when required for a specific task and reverting to standard user privileges after completion.
- **Session Monitoring**: Monitoring privileged user sessions for suspicious activity.