Access Control Policy

1. Purpose and Scope

This Access Control Policy outlines the procedures and guidelines for granting, revoking, handling, and documenting access to the organization's systems, applications, data, and facilities. This policy is designed to ensure the confidentiality, integrity, and availability of information assets while minimizing unauthorized access and potential security breaches.

2. Access Request and Approval

- All access requests must be submitted alexandra@stereopsia.brussels.
- Access requests should include the individual's name, job role, reason for access, and the specific data required.
- Access requests must be approved by the Alexandra Gérard before access is granted.
- Access permissions should be granted based on the principle of least privilege, providing only the minimum access necessary to perform the individual's job responsibilities.

3. Access Provisioning

- Authorized personnel will provision access based on approved requests.
- Access provisioning includes creating user accounts, assigning appropriate roles/permissions, and configuring access settings.
- Access provisioning should be performed promptly upon approval and follow predefined procedures to ensure accuracy and consistency.

4. Access Revocation

- Access rights should be reviewed periodically to ensure they remain necessary and appropriate.
- Access rights must be promptly revoked when an individual's job role changes, access is no longer required, or upon termination.
- Terminated employees' access rights must be revoked immediately upon notification of departure.

5. Handling Access Control Changes

- Any changes to access control permissions or roles must be documented and approved before implementation.

- Changes should follow a change management process, including proper testing and validation to avoid disruptions.

6. Documentation and Auditing

- Access control changes, approvals, revocations, and provisioning activities must be documented and maintained in a secure and centralized access control log.
- Audits of access control logs should be conducted regularly to identify unauthorized or suspicious activities.

7. Monitoring and Reporting

- Regular monitoring of access logs and activities should be performed to detect and respond to any unauthorized access attempts or anomalies.
- Incidents related to unauthorized access or breaches must be reported to the appropriate security team for investigation and resolution.

8. User Responsibilities

- Users are responsible for safeguarding their access credentials (usernames, passwords, etc.).
- Users must log out or lock their sessions when not in use to prevent unauthorized access.
- Any suspected compromise of access credentials must be reported immediately.

9. Enforcement and Non-Compliance

- Violations of this Access Control Policy will result in disciplinary actions, up to and including termination and legal action if necessary.

10. Review and Update

- This policy should be reviewed periodically to ensure its relevance and effectiveness, especially in response to changes in technology, systems, or regulations.

Conclusion

This Access Control Policy aims to maintain a secure environment by controlling access to sensitive information and resources. All employees, contractors, and stakeholders must adhere to this policy to ensure the organization's information security is upheld.