ACCESS CONTROL POLICY

Access Control Policy

Policy Number: IT.2400

Version 1

Contact: Ben Greene

Original Effective Date: 01.01.2018

Last Reviewed: 06.29.2022

Next Review/Approval Date: 06.30.2023

ACCESS CONTROL POLICY

POLICY: The control of access to Verisys information assets is a fundamental part of information security. Verisys will ensure that comprehensive controls are in place to protect the confidentiality, integrity and availability of classified data.

SCOPE: This control applies to all systems, people and processes that constitute the organization's information systems, including executive leadership, supervisors, employees, suppliers and other third parties who have access to Verisys systems.

I. Introduction:

Our policy with regard to access control must ensure that the measures we implement are appropriate to the business requirement for protection and are not unnecessarily strict. The policy must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved.

These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation
- The regulatory framework in which the organization and the system operates
- Contractual obligations to external third parties
- The threats, vulnerabilities and risks involved
- The organization's appetite for risk

This access control policy is designed to take account of the business and information security requirements of the organization.

II.Business Requirements of Access Control:

Business requirements for access control must be established as part of the requirements-gathering stage of new or significantly changed systems and services..

Information security requirements must be clearly stated within the business requirements specification document and must take account of the organization's standards established in the document *Principles for Engineering Secure Systems*.

There are a number of general principles that will be used when designing access controls for Verisys systems and services. Additional requirements may be necessary for some projects.

ACCESS CONTROL POLICY

Adherence to the following basic principles will help to keep systems secure by reducing vulnerabilities:

- *Defense in Depth* – security must not depend upon any single control but be the sum of a number of complementary controls
- *Least Privilege* – the default must be to assume that access is not required, rather than to assume that it is
- *Need to Know* – access is only granted to the information required to perform a role, and no more
- *Need to Use* – Users will only be able to access physical and logical facilities required for their role

As part of the selection of cloud service providers specifically, the following access- related considerations must be taken into account:

- User registration and deregistration functions provided
- Facilities for managing access rights to the cloud service
- To what extent access to cloud services, cloud service functions and cloud service customer data can be controlled on an as required basis
- Availability of multi-factor authentication for administrator accounts
- Procedures for the allocation of secret information such as passwords

Addressing these requirements as part of the selection process will ensure that the provisions of this policy can be met in the cloud as well as within on-premise systems.

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities.

III. User Access Management:

User access control procedures must be documented, implemented and kept up to date for each application and information system. This ensures authorized user access and prevents unauthorized access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

ACCESS CONTROL POLICY

A. User Registration and Deregistration:

A request for access to the organization's network and computer systems must first be submitted to IT Support for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorization is obtained prior to user account creation. The principle of segregation of duties will apply so that the approval of access and the assignment of permissions are performed by different people.

Each user account will have a unique username that is not shared with any other user and is associated with a specific individual i.e. not a role or job title. Generic user accounts to be used by a group of people must not be created as they provide insufficient allocation of responsibility. Exceptions to this policy must be approved and documented by the Security Engineer.

A strong temporary password must be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves the organization under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of Human Resources to request the suspension of the access rights via IT Support.

A request to remove access prior to notice of termination may be approved in exceptional circumstances. This includes cases where there is perceived to be a risk that the employee may take action that may harm the organization prior to or upon termination. This precaution will apply in the case where the individual concerned has privileged access rights.

User accounts must be suspended or disabled only and not deleted. User account names must not be reused as this may cause confusion in the event of a later investigation. Disabled user accounts must be retained for at least 12 months.

B. User Access Provisioning:

Each user must be allocated access rights and permissions that are necessary for the tasks they are expected to perform . In general, this will be role-based, whereby a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles must be maintained in line with business requirements and any changes to them must be formally authorized and controlled via the change management process.

Ad-hoc additional permissions must not be granted to user accounts outside of the group role; if such permissions are required this must be addressed as a change and formally requested in accordance with the *User Access Control Procedures*.

C. Removal or Adjustment of Access Rights:

Where an adjustment of access rights or permissions is required due to an individual changing role, this must be carried out as part of the role change. It must be ensured that access rights no longer required as part of the new role are removed from the user account.

Under no circumstances will administrators be permitted to change their own user accounts or permissions. Administration access must be approved by the Chief Operations Officer, VP of Infrastructure, or Head of Security.

D. Management of Privileged Access Rights:

Privileged access rights must be identified for each system or network and tightly controlled. In general, technical users (such as IT Support staff) will not make day to day use of user accounts with privileged access, rather a separate “admin” user account must be created and used only when the additional privileges are required. These accounts must be specific to an individual. Generic admin accounts must not be used as they provide insufficient identification of the user. As with all user accounts, Privileged accounts must follow the Least Privilege Principle.

Access to admin level permissions must only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

Users with admin level permissions are not allowed to grant permissions to their own user or admin level accounts.

The use of user accounts with privileged access in automated routines such as batch or interface jobs is prohibited. Service accounts must be used for this functionality. The credentials for service accounts must be restricted and stored in a password vault for security and continuity.

E. User Authentication for External Connections:

In line with the Network Security Policy the use of modems or wireless devices on non-company owned PCs or devices connected to the organization's network can seriously compromise the security of the network. These devices are strictly prohibited.

Where remote access to the network is required via VPN, a request must be made via IT Support. A policy of using two-factor authentication for remote access will be used in line with the principle of "something you have and something you know" in order to reduce the risk of unauthorized access from the Internet. For further information please refer to the Mobile Device Policy and Telework Policy.

F. Supplier Remote Access to the Organization Network:

Partner agencies or 3rd party suppliers must not be given details of how to access the organization's network without permission from IT Support. Any changes to supplier's connections (e.g. on termination of a contract) must be immediately sent to IT Support so that access can be updated or ceased. All permissions and access methods must be controlled by IT Support

Partners or 3rd party suppliers must contact IT Support on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and user accounts must be disabled when not in use.

G. Review of User Access Rights:

On a regular basis (at least annually) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:

- People who should not have access
- User accounts with more access than required by their role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification
- Any other issues that do not comply with this policy.

This review will be performed according to a formal procedure and any corrective actions identified and carried out.

A review of user accounts with privileged access will be carried out by the Security Team to ensure that this policy is complied with.

H. User Authentication and Password Policy:

A strong password is an essential barrier against unauthorized access.This area is often proven to be the weak link in an organization's security strategy. A variety of ways to improve the security of user authentication are available, including various forms of two-factor authentication and biometric techniques.

Verisys policy is to make use of additional authentication methods based on a risk assessment which takes into account:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

Use of multi-factor authentication methods must be justified on the basis of the above factors and securely implemented and maintained.

Whether single or multi-factor authentication is used, the quality of user passwords must be enforced in all networks and systems using the following parameters (Any exceptions to these rules must be authorized by the Security Engineer).

Parameter	**Value**
Minimum length	8
Maximum length	32
Re-use cycle	Cannot be the same as any of the previous 6 passwords

Characters Required	At least one upper case letter At least one lower case letter At least one symbol At least one number
Change Frequency	At least every 90 days
Account lockout	On 5 incorrect logon attempts
Account lockout action	Account will reset within a set period of time Account can be re-enabled by IT Support
Other controls	Password cannot contain the user name

IV. User Responsibilities:

Verisys expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems. Many high-profile security breaches have been caused by unauthorized access to user accounts resulting from passwords being stolen or guessed.

It is vital that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organization.

In order to maximize the security of our information every user must:

- Use a strong password, one which is in line with the rules set out in this policy
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or unencrypted file
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended connected to the network is locked or logged out

- Leave nothing on display that may contain access information such as login names and passwords
- Inform IT Support of any changes to their role and access requirements

Failure to comply with these requirements may result in the organization taking disciplinary action against the individual(s) concerned.

V. System and Application Access Control:

Requirements for effective access control must be addressed and appropriate measures implemented each time a new system is created or significant changes are made.

These must consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of different types of permissions (e.g. read, write, delete, execute) to objects (e.g. files, programs, menus) or to subjects (user accounts and groups)
- Provision of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls such as
    - Non-display of password as it is entered
    - Account lockout once number of incorrect logon attempts exceeds a specified threshold
    - Provide information about number of unsuccessful logon attempts and last successful logon
    - Date and time-based logon restrictions
    - Device and location logon restrictions
- User inactivity timeout
- Password management, including
    - Ability for user to change password
    - Controls over acceptable passwords
    - Password expiry
    - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Where software development is undertaken, program source code must be protected from unauthorized access in accordance with the document Secure Development Environment Guidelines.

VI. Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

DEFINITIONS: *This section is intentionally left blank.*

AFFILIATE PROCESSES/DOCUMENTS:

- Mobile Device Policy
- Telework Policy
- User Access Management Process
- Network Security Policy
- Cloud Computing Policy
- Internet Acceptable Use Policy
- Supplier Information Security Evaluation Process

REVISIONS LOG

Approval Date	Change Summary	Reason for Change
01/01/2018	Creation	
05/18/2019	Annual Review with minor revisions	Annual Review
05/04/2020	Annual Review with minor revisions	Annual Review
05/11/2021	Annual Review with minor revisions	Annual Review
06/29/2022	Annual Review - Ownership change, Updated template, Policy statement written, Affiliated documents added	Annual Review

REFERENCES

Source	Citation
ISO/IEC	27001