ACCESS CONTROL POLICY

Access Control Policy

Policy Number: IT.2400

Standard ID Number: IT.AC-1

Version: 6

Contact: Scott Jackson

Original Effective Date: 01.01.2018

Last Reviewed: 04.23.2023

Next Review/Approval Date: 04.30.2024

ACCESS CONTROL POLICY

POLICY: The control of access to Verisys' information assets is a fundamental part of information security. Verisys will ensure comprehensive controls to protect sensitive data's confidentiality, integrity and availability.

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 with access to Verisys systems.

I. Introduction:

Our policy regarding access control must ensure that the measures we implement are appropriate to the business requirement for protection and are flexible. The approach must be based on a clear understanding of the business requirements specified by the assets' owners.

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 consider the organization's business and information security requirements.

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*.

Several general principles will be used when designing access controls for Verisys systems and services. Additional requirements may be necessary for some projects. 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 several 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 necessary 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 and 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 user access lifecycle, from the initial registration of new users to the final deregistration of users who no longer require access.

User access rights must be reviewed regularly to ensure appropriate rights are still allocated. System administration accounts must only be provided to users required to perform system administration tasks.

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 submissions will be processed according to a formal procedure that ensures appropriate security checks and correct authorization is obtained before user account creation. The principle of segregation of duties will apply so that different people perform the approval of access and the assignment of permissions.

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.

A robust temporary password must be created on account setup and communicated to the user securely. The user must change the password on the first use of the account.

When employees leave the organization under normal circumstances, their access to computer systems and data must be suspended at the close of business on their last working day. Human Resources is responsible for requesting the suspension of access rights via IT Support.

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

User accounts must be suspended or disabled only and not deleted. User account names must be kept from being reused, as this may need to be clarified 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 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 created with the access permissions required by that job role.

Group roles must be maintained in line with business requirements, and any changes 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 consent is required, this must be addressed as a change and formally requested by 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 needed as part of the new role are removed from the user account.

Under no circumstances will administrators be permitted to change their user accounts or permissions. The Chief Operations Officer, VP of Infrastructure, or Head of Security must approve administration access.

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 daily use of user accounts with privileged access; instead, a separate “admin” user account must be created and used only when additional privileges are required. These accounts must be specific to an individual. Generic admin accounts must not be used as they provide insufficient user identification. 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 cannot grant their users, or admin-level accounts licensing 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, using modems or wireless devices on non-company-owned PCs or devices connected to the organization’s network can seriously compromise the network’s security. 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 align with the principle of “something you have and something you know” 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 contract termination) must be immediately sent to IT Support so that access can be updated or ceased. IT Support must control all permissions and access methods.

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:

Asset and system owners must regularly review who has access to their areas of responsibility and the level of access in place. This will be to identify the following:

- 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 follow 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 compliance with this policy.

H. User Authentication and Password Policy:

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

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

- 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)
- Are any other relevant controls in place

Multi-factor authentication methods must be justified, securely implemented, and maintained based on the above fact.

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	Only upon a risk-based event
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 username

IV. User Responsibilities:

Verisys spends significant time and money implementing adequate 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 stolen or guessed passwords.

Every user must play their part in protecting the access they have been granted and ensuring that their account is not used to harm the organization.

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 subjects (user accounts and groups)
- Provision of menu options and data according to the user account and its permission levels
- User account administration, including the ability to disable and delete accounts
- User login controls such as
    - Non-display of password as it is entered
    - Account lockout once the number of incorrect logon attempts exceeds a specified threshold
    - Provide information about the number of unsuccessful login attempts and the last successful logon
    - Date and time-based login restrictions
    - Device and location login restrictions
- User inactivity timeout
- Password management, including
    - The ability for users to change password
    - Controls over acceptable passwords
    - Password expiry
    - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful login attempts, object access, and account administration activities

Where software development is undertaken, the document Secure Development Environment Guidelines must protect program source code from unauthorized access.

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	Compliance
05/04/2020	Annual Review with minor revisions	Compliance
05/11/2021	Annual Review with minor revisions	Compliance
06/29/2022	Annual Review - Ownership change, Updated template, Policy statement written, Affiliated documents added	Compliance
04/20/2023	Annual Review – minor cleanup, changed “change frequency” parameter in table to “only upon a risk-based event” to align with the NIST standard update regarding password update frequency.	Compliance

REFERENCES

Source	Citation
ISO/IEC	27001