Access Control Policy and Procedures

Objectives

This policy establishes procedures for managing risks from user account management, access enforcement and monitoring, separation of duties, and the establishment of an access control program. Access control policies are high level requirements that specify how access is managed and who may access information under what circumstances.

The access control program helps Sonsray implement security best practices with regards to logical security and account management. These standards are designed to minimize the potential exposure of Sonsray to damages which may result from unauthorized use of Sonsray resources, and to protect confidential information from unauthorized or unintended disclosure.

Policy Statement

The scope of this policy is applicable to all data and records used and owned by Sonsray. Any information, not specifically identified as the property of other parties, that is transmitted or stored on Sonsray IT resources (including e-mail, messages, and files) is the property of Sonsray. All Users (Employees, contractors, vendors, temps, government representatives, auditors or others) of IT resources are responsible for adhering to this policy. Sonsray has provided access to company electronic communications systems, networks, and devices, collectively with Employees referred to as “Authorized Users.”

These standards include the minimum requirements. It is acceptable to implement measures that are more stringent than what is documented in the standards. Exceeding the minimum requirements does not necessitate a security exception. Where requirements cannot be met, a Security Exception must be filed, reported and acknowledged by Sonsray IT Management. The exception report must describe compensating security controls.

Continued on next page

Access Control Policy and Procedures, Continued

Definition of Terms

Below are the terms used in this document.

Term	Definition
Access Control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., offices, data centers, factories, labs).
Access Control Policy	The set of rules that define the conditions under which an access may take place.
Account Management	The process of requesting, establishing, issuing, and closing User accounts. Tracking Users and their respective access authorizations, and managing these functions.
System Use Notification	A banner display for Users with message before granting access to the system that provides privacy and security notices consistent with applicable federal laws.
Session Lock	The time-period of inactivity in a computer. Prevents further access to the system by initiating a session lock of inactivity or upon receiving a request from a User.
Permission	An authorization to perform some action on the system. In most computer security literature, the term permission refers to some combination of object and operation. An operation used on two different objects represents two distinct permissions, and similarly, two different operations applied to a single object represent two distinct permissions.
Privileged User	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Administrators are typically considered privileged users.
Wireless Access	A device that acts as a conduit to connect wireless communication devices together to allow them to communicate and create a wireless network.

Responsibilities

Sonsray manages access in accordance with internal policy and best practices described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Information Security.

Continued on next page

Access Control Policy and Procedures, Continued

Sonsray's Policy Standards

The following subsections outline the standards that constitute Sonsray policy. Sonsray IT Team must support and adhere to the following:

- □ Determine the allowed activities of legitimate Users, mediating every attempt by a User to access a resource in the system.
- □ Document verified Users and terminate unused accounts.
- □ Limit Users access to file permissions or objects
- □ Assign Users to roles to enforce constraints. Membership of one role may prevent the User from being a member of one or more other roles.
- □ Implement least privilege for all Users to identify specific Users with need-to-know access or restrict Users to a domain:
  - ▪ Administrative rights will not be granted to normal end Users as these rights elevate the risk to the organization.
  - ▪ If an end User believes they need administrative rights to their assigned device to utilize a specific business software application, a User Rights Matrix should be submitted. This request will then be evaluated by the IT Director. Upon approval by the end user's management and the IT Director, the IT team will work with the end User to determine if an alternative rights level or alternative software can be substituted for full administrative rights.
  - ▪ Administrative machine rights may be granted by exception only and only used by the end User specifically for the intended exception purpose.
  - ▪ Abuse of administrative rights and/or attempts to circumvent security measures implemented by Sonsray is a violation of this policy and may result in administrative rights being revoked and/or disciplinary action(s).

Continued on next page

Access Control Policy and Procedures, Continued

Security Training Program

The IT Director is responsible for the creation of a Security Training Program and for providing that information to Sonsray Management and Users. The Security Training Program material should include current security related information, procedures, and leading practices that familiarize Users with a secure approach to operating information systems and handling data. The Sonsray Management team should provide this information to all Users as part of the initial User's orientation program and annually as the program material is updated. The Sonsray Management Team should promote these secure practices at all times. The IT Director will be responsible for the administration of the Security Training Program.

Role Based Access Control

Role-Based Access Control must be enforced. That is all users, administrators, and/or applications having the same job function will have the same access role. An individual or application may have multiple access roles if they have multiple job functions. Job functions and access roles will be created and maintained by each application owner.

Creating and Defining a New Role	The creation of a new access role must undergo a change control process and must be approved by the owner of the data that will be accessed.
Least Privilege Principle	The least privilege principle must be enforced. That is, a user must not be given any more privilege than necessary to perform a user's job as defined by business need. Access to restricted or highly confidential data, as defined by the Data Classification Standard within Sonsray's Critical Files and Folders Process, must be strictly controlled by need-to-know. For data that is classified as confidential, a user may be given access more broadly to include data that may be needed in the future. Normal users, i.e. non-administrators, shall be issued accounts which do not have privileges to access security relevant functions on information. Security functions include, for example, establishing system accounts, configuring access authorization (i.e. permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

Continued on next page

Access Control Policy and Procedures, Continued

Role Based Access Control, cont.

Separation of Duties	Separation of duty relations must be used to avoid conflict of interest. Conflict of interest in a role-based system may arise as a result of a user gaining authorization for permissions associated with conflicting roles (e.g. No single role can execute the duties to both establish a new vendor and to authorize vendor payment). With respect to IT systems, a change to the system (creating system account, changing functionality, etc.) may not be requested, approved, and implemented by the same individual. In addition, the normal administrator of a system shall not also conduct audits of the security control of the system. Company conducts a periodic review of assigned user privileges necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, Company will take appropriate corrective actions. All Company applications and systems must enforce separation of duties as applicable. Roles that have been specified as mutually exclusive should not be included together in a user's set of authorized roles. Individuals needing both user and administrator privileges on an Active Directory integrated system must request a separate administrator account and have administrative privileges attached to their administrator Enterprise ID. Generic IDs (Service Accounts) will be justified, approved and periodically reviewed by IT Management for specific use. Where possible, interactive logon shall be disabled for service accounts.

Continued on next page

Access Control Policy and Procedures, Continued

Multifactor Authentication (MFA)

MFA must be used to protect networks and information systems containing Controlled Unclassified Information. Sonsray has determined this applies to the DFARS network segment.

Where MFA is required, the factors must meet two of the three standards:

- □ something you know (pin/password)
- □ something you have (token/certificate)
- □ something you are (fingerprint/iris scan)

If a pin is used as something you know, the pin must be at least 6 digits in length. If passwords are used, they must meet the requirements outlined in the Passwords section.

Sonsray uses either a one-time password, Token-based system, or certificate based.

Passwords

Sonsray must document and manage password usage, strength requirements, changing and control through formal processes.

- □ Passwords should always be encrypted when held in storage for any significant period of time. Passwords are encrypted using a software with encryption of at least AES-256 level.

- □ Passwords should always be encrypted in transit. In general, systems shall send a hashed representation of a password for authentication. Where this is not possible, an encrypted channel must be used, i.e. SSH/SSL.

- □ Passwords should not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.

Continued on next page

Access Control Policy and Procedures, Continued

Passwords, continued

☐ The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

☐ The initial passwords issued to Users should be valid only for the involved User's first on-line session. At that time, the User must be forced to choose another password before any other work can be done.

☐ Authorized personnel should only disclose passwords if a new User-ID is being assigned, if the involved User has forgotten or misplaced a password, or if the involved User is otherwise locked out of his or her User-ID. Care should be exercised to ensure that the involved User is verified to avoid a security breach through “social engineering.”

☐ An encrypted history of previous passwords should be maintained for Network equipment and workstations. This history file should be employed to prevent Users from reusing recent passwords. The history file should minimally contain the last 24 passwords for each User-ID.

☐ All Users should be automatically forced to change their passwords at least once every 100 days. Any deviation from this must be reviewed and acknowledged by the IT Director on an annual basis.

☐ An administrative account that is only used by software or the system and not by personnel may be excluded from the 100-day lifetime limitation.

☐ All application service account passwords must be stored in encrypted password databases. These passwords must be changed whenever an authorized User’s access is terminated.

☐ Four (4) consecutive unsuccessful login attempts will trigger the Network to automatically lock the offending account for either a reasonable period of time or until it is determined that the account should be unlocked.

Continued on next page

Access Control Policy and Procedures, Continued

Password Complexity

Complex password specification for Sonsray:

- □ Have at least 8 characters
- □ Contain a character from at least three of the following four categories:
    - ▪ English uppercase alphabet characters (A-Z)
    - ▪ English lowercase alphabet characters (a-z)
    - ▪ Base 10 digits (0-9)
    - ▪ Non-alphanumeric characters, for example, ~! @#$%A&*_-+='|\(){}[]:;"'<>.?/
- □ Not contain any 3-character string that is contained in the User ID
- □ Application passwords and Application database passwords (where supported) should conform to the network password standards
  NOTE: Updated Password Requirements, per NIST SP 800-63, Appendix A - Max length increased to 64 or more. All printable characters allowed, including space. Complexity decreased to must include one upper/number/symbol. Password should be compared to dictionaries and lists of easily guessed and previously compromised. Passwords should only be changed following a known or potential compromise.

Continued on next page

Access Control Policy and Procedures, Continued

Privacy and Security Notice

The notice is a warning against unauthorized use of the computer and indicates that such use implies consent to all relevant Sonsray policies. A system use notice should be displayed for Users to identify the system as a Sonsray system. The system use notice must state the following or something similar:

> *"NOTICE:"*
>
> *This computer system is the property of Sonsray ("Company"). It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with Sonsray's Acceptable Use Policy ("AUP"), and all IT Policies. Users have no personal privacy rights in any materials they place, view, access, or transmit on this system. The Company complies with state and federal law regarding certain legally protected confidential information, but makes no representation that any uses of this system will be private or confidential. By using this system, the user consents to file and/or data interception, monitoring, recording, copying, auditing, inspection, deletion and/or disclosure at the discretion of authorized Company personnel. Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions as set forth in the Company's AUP and IT Policies.*

Continued on next page

Access Control Policy and Procedures, Continued

Access

Access to both Company internal and external networked services must be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of those network services. The following requirements must be followed:

☐ Only authorized users have access to Company networks.

☐ Authentication is required, where technically possible, when connecting to the LAN.

☐ Physical access to the diagnostic ports should be strictly controlled. Diagnostic ports should not be available outside of a secured room or location.

☐ Any user device connecting to the Company network (either in-office or remote) must have installed and functioning all required security software as defined by the applicable Company standard (e.g., antivirus, personal firewall, hard drive encryption, etc.).

☐ Users may not connect to multiple networks simultaneously when connected to the Company network.

Remote Access	Positive identification for Users originating from external connections to company internal networks via value added networks (i.e. Remote Desktop, VNC, etc.), public networks (i.e. Internet), or any other external system must be through a secure connection, such as a virtual private network. Sonsray must report and update remote access procedures to provide suitable protections through identification, authentication, and encryption methods.

Continued on next page

Access Control Policy and Procedures, Continued

Access, cont.

Standard Network Access	All access requests for new users must be submitted on a New Hire Form or the equivalent, which should include the user information, required access levels, and business management approval. All access requests for a contractor, consultant, temp, intern, or other type of temporary User must be submitted on a New Hire Form where the appropriate checkbox shall indicate the start and finish date of the temporary User. This will allow the Support Center to set the temporary User's Network access to automatically expire in accordance with the date submitted on request. The maximum time allowed for a temporary User account is 90 days. Extensions will require a Security Access Form with the approval of the IT Director. Sonsray managers will submit an Employee Termination Form to remove the temporary User permissions/access as soon as the permissions/access are no longer needed.
Temporary Network Access	All access requests for a contractor, consultant, temp, intern, or other type of temporary User must be submitted on a New Hire Form where the appropriate checkbox shall indicate the start and finish date of the temporary User. This will allow the Support Center to set the temporary User's Network access to automatically expire in accordance with the date submitted on request. The maximum time allowed for a temporary User account is 90 days. Extensions will require a Security Access Form with the approval of the IT Director. Sonsray managers will submit an Employee Termination Request to remove the temporary User permissions/access as soon as the permissions/access are no longer needed.
User Transfers and Changes in User Access	All requests for changes in user access levels must be submitted on a Security Access Request Form or the equivalent, this should include the user's old access and rights to be removed, the user's new required access levels, and business management approval. Access changes will take effect within 30 days of business management approval.

Continued on next page

Access Control Policy and Procedures, Continued

Access, cont.

Termination	Upon the termination of the services of a user, the user’s manager or assigned HR personnel must submit a completed IT Access Termination request to start the access termination for the employee. This form should be submitted before the date of user termination if practical. Accounts must be terminated within 72 hours of the User’s last day. If a termination is high-risk, the User’s access must be terminated immediately. Usernames shall not be reused for at least 90 days after termination. Accounts will be placed in a disabled status preventing their reuse.

Audit and Monitor

Sonsray must address and update appropriate logging and monitoring functionality. Sonsray will review all audit records on Employees who work in the office and who remotes into the network (ex: User activity logs) for inappropriate activities in accordance with organizational procedures. Sonsray will use audit records for investigations of any unusual information system-related activities and periodically review changes to access authorizations. The organization will review daily the activities of Users with significant information system roles and responsibilities.

The administrator of a system or change manager is not responsible for auditing the system or change.

Network User accounts will be monitored for inactivity as well. Any Network User account that has been inactive for more than 45 days will be disabled and the User’s manager (if known) will be notified. If the Network User’s account has been disabled for more than 90 days, the Network User account and all access for that account will be deleted. Exceptions will require a Security Access Form with the approval of the IT Director and will be periodically reviewed to confirm ongoing exception status.

On a monthly basis, the IT administrator will review the IT Request Form to ensure the terminated User’s network and application access is disabled.

Continued on next page

Access Control Policy and Procedures, Continued

Review of Administrator User Access Rights

To maintain effective control over access to data and information services, an IT Administrator must conduct and document a formal review process on a quarterly basis.

When performing the administrator access review, the following items are part of the review: Network Operating Systems, Financial Applications, Firewalls, Wireless Networks and e-Mail System.

Enforcement

All Employees are responsible for compliance with this policy and associated guidelines as a condition of employment, contract, or practice at Sonsray. A statement acknowledging understanding of these policies and pledging compliance is signed by all users of information at the beginning of their association with Sonsray and/or prior to being granted access to any computer resources.

If an Employee is found violating a policy, a warning is given to the individual and recorded in the Employee's personnel file. Further failure to comply may result in disciplinary action up to and including termination of employment or revocation of privileges.

Revision Control History

Below is the revision history for this policy.

Revision Date	Revised By	Revision Status	Executive Approval, Date
2/15/2023	Rachelle McKenzie	New	8/17/2023
2/24/2023	James Martinez	Grammar, Spelling Check p.3, 11	3/6/2023