ACCESS CONTROL POLICY

SRI LANKA CERT|CC

An Agency under the Ministry of Technology

Draft - Version 1.0

December 2020

Access Control Policy
[Draft]

1. Objective of the Policy

The primary objective of this document is to provide guidelines for government organizations to develop Access Control Policy to protect their information assets from unauthorized modification, disclosure or destruction and to ensure that confidentiality, integrity and accuracy of the information assets is maintained.

This policy aims to ensure that, by having the appropriate access controls in place, the right information is accessible by the right people at the right time and that access to information, in all forms, is appropriately managed and periodically audited.

2. Scope of the Policy

Logical Access control focuses on the user accounts management and users' passwords management where the applied controls either prevent or allow access to resources once a user's identity already has been established.

Access control policy should apply the principle of least privilege and be on the basis of Need-to-know and Need-to-Access principle. In the need-to-know principle, the granting access rights to a user to access information shall be only based on the task that user performs (user is given the least amount of data required to perform his/her job). In the Need-to-use basis user is only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) where user need to perform the task/job/role.

This policy shall be applied to all the staff/employees of the government organization and third parties including contractors, consultants, temporary workers, or vendor personnel.

3. User Registration and Assigning User IDs

3.1. All information systems, servers, networking devices, applications, or any other device or application must require identification and authentication through passwords, pass-phrases, one-time passwords and/or similar password mechanisms.

3.2. The organization should follow a formal user registration and de-registration process in order to grant access (or revoke) to information assets/systems.

3.3. Registration (or deregistration) of users to access the systems shall be done only by two level of authorizations, namely, (1) information asset owner, and

(2) CIO/ISO. Users shall only provide access to the organization systems after the full completion of authorization procedures.

3.4. CIO/ISO shall maintain a formal record of all registered users for each information asset.

3.5. All registered users must be provided with a written statement of their access rights and terms and conditions for usage of these rights, which should be formally accepted.

3.6. The allocation of secret authentication information shall be controlled through a formal management process to protect the identities and manage the credentials for authorized users.

3.7. All users of information assets must have a unique user ID to access the organization's information assets/systems.

3.8. The user ID naming convention must be consistent and documented.

3.9. Redundant user ID's must not be re-issued to new users.

3.10. User Accounts that are inactive for a maximum 90 days must be disabled.

3.11. User IDs and the accounts of the employees must be removed immediately upon their termination, through a de-registration process. Removing such accounts should not take more than one business day.

3.12. Accounts of users transferred to different department/section/or promoted must be reviewed by the users reporting manager, information asset owner and ISO prior to updating access rights.

3.13. Access to organization information assets and activation of user accounts must only be in effect when the individual is actively performing service for the organization.

3.14. Access to organization information assets and activation of user accounts for third parties including contractors, consultants, temporary workers, or vendor personnel must only be in effect when the individual is actively performing service for the organization.

3.15. Allocation of user accounts and access rights and updating of users access rights shall be documented and the documents shall be retained for a defined period of time.

3.16. Users are responsible and liable for all actions performed by using their user ID(s) and password(s).

3.17. Each user must terminate active sessions when activities are finished.

3.18. Users must log off from their user accounts after completion of their tasks.

4. Privilege Accounts Management

4.1. Privileged access request should be provided after three levels of approval – (1) the users Reporting Manager, (2) information assets owner, and (3) ISO/CIO.

4.2. The allocation and use of privileged access rights shall be restricted and controlled. Access permissions shall be managed, incorporating the principles of least privilege and separation of duties.

4.3. A system administrator emergency ID and password shall be maintained in a sealed envelope in a secured area. In case the ID is used, the password should be changed upon completion of the task and the ID and new password shall be sealed and securely stored again.

4.4. In case the administration of a specific platform, such as Unix, cannot be effectively supported in the manner described, an alternative process should be set up to provide privileged functions in routine situations.

4.5. All user privilege rights must be reevaluated and reviewed periodically.

5. Shared User Account Management

5.1. Access to the shared user accounts should be granted after three levels of approval – (1) the users Reporting Manager, (2) information assets owner, and (3) ISO/CIO.

5.2. Shared user accounts should be assigned with least privileges.

5.3. The list of shared account users should be documented.

5.4. Logging activities of the users should be logged and reviewed.

5.5. Passwords of the shared accounts should be changed on a regular basis.

5.6. Shared user accounts that have system-level privileges must have a unique password from all other accounts held by that user.

6. Validation of User Accounts

6.1. Each user account should be reevaluated by the ISO/CIO and information asset owner at a fixed frequency - preferably 6 months for normal user accounts and 3 months for privileged user accounts.

6.2. At a minimum, non-validated accounts should be terminated/locked in one working day (at a maximum, five working days).

7. User Transfers and Terminations

7.1. In the event of a user getting transferred to different department/section/ or promoted, the user's manager and IAO should have authorized access to the Information Asset and ISO must update user's access privileges. At a minimum, updating privileges shall be done within minimum 24 hours.

7.2. Upon the termination of employment, User ID should be removed immediately. At a minimum, access termination should be done in 24 hours.

7.3. Removal and updating of user accounts and access rights shall be documented and maintained for a pre-defined time period.

8. User Password Management

8.1. Passwords must be regarded as confidential information and must not be disclosed to any other person except in accordance with the organization's password management procedures for safekeeping of passwords. Government organizations should use multi-factor authentication approach for critical systems and devices.

8.2. Passwords must not be revealed in conversations, inserted into e-mail messages (where encryption options are unavailable) or other forms of electronic communication.

8.3. All users must be forced to change their temporary passwords on first logon.

8.4. All passwords must be changed after predetermined intervals: 30 days for privileged access IDs and 90 days for regular access.

8.5. Passwords must be checked to ensure that they are not identical to any of a predetermined number of previous passwords for the same account.

8.6. All user-level and system-level passwords composition must conform, at a minimum, to the following guidelines:

8.6.1. Passwords must contain both upper and lower-case characters (e.g., a-Z)
8.6.2. Passwords must have digits, special characters and letters (e.g., 0-9, !@#$%^&*,Ab)
8.6.3. Passwords must be at least eight characters long.
8.6.4. Passwords must not be a word in any language, slang, dialect, jargon, etc.
8.6.5. Passwords must not be based on personal information, names of family, friends, relations, colleagues, etc.

8.7. Passwords must not be written down, stored on any information system or storage device except in accordance with the government organization's password management procedures for safekeeping of passwords.

8.8. Passwords shall not be transmitted or stored in clear text

8.9. Passwords shall be conveyed verbally in person, in hardcopy sealed envelope with confirmation of receipt, etc. Wherever strong encryption options are available, conveying of initial temporary passwords via e-mail should be considered.

8.10. Passwords shall be protected at-rest and in-transit using encryption.

8.11. Passwords are not to be displayed on the screen when entered.

8.12. In case of forgotten passwords, temporary passwords should be issued only after positive identification of the user as prescribed in the Section XYZ.

8.13. The organization's information systems must be configured (where this is possible) to lock the user ID and prevent user access to the information system where an incorrect password has been used for three times in sequence for privileged accounts and five times in sequence for other accounts.

8.14. Locked out user accounts must be reactivated after positive identification of the user and following a defined formal procedure to reactivate locked out user accounts. Re-activation shall be approved by ISO/CIO, Information Assets Owner, and users reporting manager.

8.15. An encrypted history file should be maintained and should, at a minimum, retain the last 13 passwords for each user ID. The users must be educated and made aware of password confidentiality to hinder displaying and printing passwords.

8.16. Password files should be stored in an encrypted form within the application, separately from the application data, to prevent any unauthorized access.

8.17. Vendors' default passwords should not be retained in the systems following the installation of any application or operating system software.

9. Access to Networks and Network Services

9.1. Access to networks and network services shall be controlled on the basis of business and security requirements, and access control rules defined for each network.

9.2. Remote user access to the organization's networks shall be subject to appropriate user authentication methods.

9.3. When accessing office network and data from external sources, ensure that access is through the (Virtual Private Network) VPN service provided by your organization. This ensures secure transmission of data.

9.4. Internal networks must be segregated from the external network with different perimeter security controls on each of the networks.

9.5. The connectivity between internal and external networks must be controlled.

10. Operating System Access Control

10.1. The terminal logon procedure must disclose a minimum amount of information about the system.

10.2. Password management system shall suspend the user ID after minimum five consecutive unsuccessful login attempts.

10.3. Terminal time out or workstation locking shall be enabled to lock the terminals, after a defined period of inactivity.

10.4. To reset the user ID after a suspension, an approval shall be received from the user's supervisor.

10.5. A legal banner must appear on all organization systems prior to login to the system warning that the system should only be accessed by authorized users.

10.6. The logon procedure must not identify the system or application until the logon process has been successfully completed.

10.7. Help messages shall not be provided to users during the log-on procedure which would aid an unauthorized user.

10.8. The system must validate the logon information only on completion of all input data.

10.9. After a rejected logon attempt, the logon procedures must terminate.

10.10. The logon procedure must not explain which piece of information (the user ID or password) was the reason for the logon termination.

10.11. The logon procedures must set a maximum number of five attempts and maximum time allowed for the logon process.

10.12. On successful completion of logon, the logon procedures must display the date/time of the previous successful logon, and the number and date/time of unsuccessful logon attempts since the last successful logon.

10.13. Access to and use of system programs must be restricted and controlled.

10.14. Use of system programs must be limited to authorized individuals.

10.15. All actions performed by an individual on system programs must be logged.

10.16. All unnecessary system utilities and software, including compiler programs, must be removed.

10.17. Access to system tools that have the capability to override system and application controls are restricted for all users, except those with documented authorization.

10.18. System tools shall be protected against unauthorized access.

10.19. Access to system utilities shall be limited to the minimum practical number of authorized individuals.

10.20. Access to all system utilities shall be logged to facilitate the identification of inappropriate use.

10.21. Ad hoc use of system utilities shall not be allowed unless specifically authorized.

11. Application Access Control

11.1. Access to the organization's information resources and applications must be limited to users who require them to perform their job tasks.

11.2. All users must have controlled access to all information resources and business applications of the organization, in accordance with need to know and need to use basis. Controlled access would include but not be limited to Read, Write, Modify, Execute, and/or Full control.

11.3. All applications must require each end user to have their own unique user ID to login.

11.4. Application timeout standards shall be enforced and require a user to re-enter a password/phrase after a period of inactivity to regain access to their application.

11.5. Emergency or Nonstandard Access privileges shall be granted on a temporary basis and require explanatory documentation, and approval from the ISO/CIO. ISO/CIO shall be responsible for the timely removal of the temporary access. A record of all these exception items shall be maintained for reviews.

11.6. All unsuccessful login attempts to critical servers must be recorded, investigated, and if necessary, escalated to management.

12. Compliance & Enforcement

a. Compliance

12.1. Compliance with this Procedure is mandatory. The ISO/CIO must ensure continuous compliance monitoring of all relevant IT processes. Compliance with this Policy will be subject to periodic review by the IT department of the Organization.

12.2. Violations of the policies, standards and procedures of organization will result in corrective/preventive actions by management. Disciplinary actions will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to: Loss of access privileges to information assets and action taken recommended by the Head of the Organization. Other actions as deemed appropriate by management, Human Resources, and the Admin/Legal Department.

b. Enforcement

12.3. Requested waivers must be formally submitted to the IT Department, including business justification and benefits attributed by the waiver, and must be approved by the<AUTHORIZED PERSONNEL, depending on the criticality.

12.4. The waiver shall only be used in exceptional situations where the laid down procedure cannot be enforced and when communicating non-compliance with the policy for a specific period of time as determined by the IT department (subject to a maximum period of six months).

12.5. At the completion of the agreed time period the business requirement for the waiver shall be reassessed and re-approved, if necessary. No policy/procedure shall be provided waiver for more than three consecutive terms.

12.6. In the event of three consecutive policy exceptions granted, the policy should be immediately automatically reviewed.

Access Control Policy Check List

#	Task	Compliance
1	The organization follows a formal user registration and de-registration process in order to grant or revoke access to information assets/systems.	
2	Access to all information systems, servers, networking devices, applications, or any other device or application are protected and authenticated through passwords, pass-phrases, one-time passwords and/or similar password mechanisms.	
3	User registration, de-registration and providing access to the systems are done after the full completion of authorization procedures by two levels namely, (1) information asset owner, and (2) CIO/ISO.	
4	CIO/ISO maintains a formal record of all registered users for each information asset.	
5	Registered users are provided with a written statement of their access rights and terms and conditions for usage of these rights, and it has been formally accepted by the user.	
6	All users of information assets have a unique user ID to access the organization's information assets/systems.	
7	The organization has a consistent user ID naming convention which is documented.	
8	Redundant user ID's are not re-issued to new users.	
9	User Accounts that are inactive for a maximum 90 days are disabled.	
10	Terminated employee's user IDs and the accounts are removed within one business day of their termination, through a de-registration process.	
11	Accounts of users transferred to different department/section/or promoted are reviewed by the users reporting manager, information asset owner and ISO prior to updating access rights.	
12	Access to information assets and activation of user accounts for third parties including contractors, consultants, temporary workers, or vendor personnel are only be in effect when the individual is actively performing service for the organization.	
13	Allocation of user accounts and access rights and updating of users access rights are documented and the documents are retained for a defined period of time.	
14	Privileged access is provided after three levels of approval – (1) the users Reporting Manager, (2) information assets owner, and (3) ISO/CIO.	
15	The allocation and use of privileged access rights are restricted and controlled.	
16	Access permissions are managed, incorporating the principles of least privilege and separation of duties.	
17	System administrator emergency ID and password are maintained in a sealed envelope in a secured area.	
18	Whenever the ID is used, the password is changed upon completion of the task and the ID and new password are sealed and securely stored again.	

19	In case the administration of a specific platform, such as Unix, cannot be effectively supported an alternative process is set up to provide privileged functions in routine situations.	
20	All user privilege rights are reevaluated and reviewed periodically.	
21	Access to the shared user accounts are granted after three levels of approval – (1) the users Reporting Manager, (2) information assets owner, and (3) ISO/CIO.	
22	Shared user accounts are assigned with least privileges.	
23	The list of shared account users is documented.	
24	Logging activities of the users are logged and reviewed.	
25	Passwords of the shared accounts are changed on a regular basis.	
26	Shared user accounts that have system-level privileges have unique passwords from all other accounts held by that user.	
27	Each user account is reevaluated by the ISO/CIO and information asset owner at a fixed frequency - preferably 6 months for normal user accounts and 3 months for privileged user accounts.	
28	Non-validated accounts are terminated/locked in within one working day minimum (at a maximum, five working days).	
29	In the event of a user transferred to different department/section/ or promoted, the user's manager and IAO have authorized access to the Information Asset and ISO update user's access privileges within minimum 24 hours.	
30	User ID is removed immediately upon the termination of employment and access termination is done within 24 hours.	
31	Removal and updating of user accounts and access rights are documented and maintained for a pre-defined time period.	
32	Passwords are regarded as confidential information and not disclosed to any other person except in accordance with the organization's password management procedures for safekeeping of passwords.	
33	Multi-factor authentication approach is used for critical systems and devices.	
34	Passwords are not revealed in conversations, inserted into e-mail messages or other forms of electronic communication.	
35	All users change their temporary passwords on first logon.	
36	All passwords are changed after predetermined intervals: 30 days for privileged access IDs and 90 days for regular access.	
37	Passwords are not identical to any of a predetermined number of previous passwords for the same account.	
38	All user-level and system-level passwords composition conform to the given guidelines.	
39	Passwords are not transmitted or stored in clear text.	
40	Passwords are conveyed verbally in person, in hardcopy sealed envelope with confirmation of receipt, etc.	
41	Passwords are not to be displayed on the screen when entered.	
42	In case of forgotten passwords, temporary passwords are issued only after positive identification of the user.	
43	Information systems are configured (where this is possible) to lock the user ID and prevent user access to the information system where an	

	incorrect password has been used for three times in sequence for privileged accounts and five times in sequence for other accounts.	
44	Locked out user accounts are reactivated only after positive identification of the user and following a defined formal procedure to reactivate locked out user accounts. Re-activation is approved by ISO/CIO, Information Assets Owner, and users reporting manager.	
45	An encrypted history file is maintained and at a minimum, last 13 passwords for each user ID are retained.	
46	Password files are stored in an encrypted form within the application, separately from the application data.	
47	Vendors' default passwords are not retained in the systems following the installation of any application or operating system software.	
48	Access to networks and network services are controlled on the basis of business and security requirements, and access control rules defined for each network.	
49	Remote user access to the organization's networks is subject to appropriate user authentication methods.	
50	When accessing office network and data from external sources, access is only provided through the (Virtual Private Network) VPN service of the organization.	
51	Internal networks are segregated from the external network with different perimeter security controls on each of the networks.	
52	The connectivity between internal and external networks are controlled.	
53	The terminal logon procedure discloses a minimum amount of information about the system.	
54	Password management system suspends the user ID after minimum five consecutive unsuccessful login attempts.	
55	Terminal time out or workstation locking is enabled to lock the terminals, after a defined period of inactivity.	
56	Reset of the user ID after a suspension, is done only after an approval received from the user's supervisor.	
57	A legal banner displayed on all systems prior to login to the system warning that the system should only be accessed by authorized users.	
58	The logon procedure does not identify the system or application until the logon process has been successfully completed.	
59	Help messages are not provided to users during the log-on procedure.	
60	The system validates the logon information only on completion of all input data.	
61	After a rejected logon attempt, the logon procedures terminate.	
62	The logon procedure does not explain which piece of information (the user ID or password) was the reason for the logon termination.	
63	The logon procedures set a maximum number of five attempts and maximum time allowed for the logon process.	
64	On successful completion of logon, the logon procedures display the date/time of the previous successful logon, and the number and date/time of unsuccessful logon attempts since the last successful logon.	
65	Access to and use of system programs are restricted and controlled.	
66	Use of system programs are limited to authorized individuals.	

67	All actions performed by an individual on system programs are logged.	
68	All unnecessary system utilities and software, including compiler programs, are removed.	
69	Access to system tools that have the capability to override system and application controls are restricted for all users, except those with documented authorization.	
70	System tools are protected against unauthorized access.	
71	Access to system utilities is limited to the minimum practical number of authorized individuals.	
72	Access to all system utilities is logged to facilitate the identification of inappropriate use.	
73	Ad hoc use of system utilities is not allowed unless specifically authorized.	
74	Access to the organization's information resources and applications is limited to users who require them to perform their job tasks.	
75	All users have controlled access to all information resources and business applications of the organization, in accordance with need to know and need to use basis.	
76	All applications have an unique login user ID for each end user.	
77	Application timeout standards are enforced and require a user to re-enter a password/phrase after a period of inactivity to regain access to their application.	
78	Emergency or Nonstandard Access privileges that are granted on a temporary basis are properly documented with explanatory documentation, and approval from the ISO/CIO.	
79	All unsuccessful login attempts to critical servers are recorded, investigated, escalated to management if necessary.	