ACCESS CONTROL POLICY

April 2020

IL7
SECURITY

Contents

1 Overview

Access control is a foundational building block of any cyber security regime, as it is designed to ensure that only appropriately authorised individuals have access to systems, services and information, thereby aiming to limit the scope for the compromise of confidentiality, integrity or availability to an irreducible minimum.

Access control provides the first line of defence against a significant majority of cyber-attacks and is fundamental in limiting the ability of attackers to further compromise a system or information in the event that they gain some limited access.

Therefore, a robust access control strategy is very important in maintaining a positive cyber security posture.

1.1 Purpose

This document defines the access control requirements for the organisation’s projects and personnel to implement in order that they can develop secure systems and information accessed is limited to the business needs of the organisation.

1.2 Scope

This policy applies to all systems operated within the organisation, including all networks, services and applications. The scope does not cover physical access control, for example to buildings, rooms and physical information.

1.3 Applicability

This policy applies to all IL7 staff and systems, including third party services.

2 Access Control Policy

2.1 Policy and Controls

This policy is written to ensure that the outcomes of the following Cyber Security Principles are met;

- SP06 Operational Security (Ref [1])
- SP15 Access Control (Ref [2])

This policy is one of several that are required to support principles above.

This policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 [3]:

XX-XX	NIST Controls
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-8	System Use Notification
AC-9	Previous Logon (Access) Notification
AC-10	Concurrent Session Control
AC-11a	Session Lock
AC-11b	Session Lock
AC-16	Security Attributes
AC-20	Use of External Information Systems
AC-24	Access Control Decisions
AC-25	Reference Monitor
CM-5	Access Restrictions for Change
MA-3 (4)	Restricted Tool Use
PS-5	Personnel Transfer
PS-6	Access Agreements
SC-2	Application Partitioning
SC-43	Usage Restrictions

This policy document supports IL7 compliance with NIST Control AC-1 – Access Control Policy and Procedures.

This policy forms one element of the implementation of a robust Identity and Access Management (IdAM) Framework and hence must be read and implemented in concert with the Authentication and Account Management Policies, Refs [4] and [5] respectively.

3 General Requirements

Management, Systems Designers and Administrators shall:

Policy ID	Policy Requirement
1.1.1	Implement logical access control mechanisms to all systems, services and devices used by IL7, including those delivered by third-parties. [NIST AC-3]
1.1.2	Align the compliance with the requirements of this policy with the requirements of the Account Management Policy (Ref [5]), particularly requirements surrounding the need for: • Identifying types of User accounts and access permissions required to perform a business/job function; • Assignment of Account Managers to manage account allocation and privilege allocation; • Defined 'entry requirements' for the issue of accounts and permissions; • Alignment with IL7 Joiners, Movers and Leavers, and Change processes.
1.1.3	In all cases, follow the principle of Least Privilege, where access or permissions are provided to only those services and functions that are required for an entity (individual, service, system/application component or process) to perform their assigned function. [NIST AC-6] Care must be given to the allocation of privileges to avoid any conflict of interest e.g. ensuring that administrators cannot provide themselves with the ability to further raise their privilege.
1.1.4	By default, implement a system of Role Based Access Control (RBAC) to manage privileges. If, for technical purposes or where determined by a risk assessment, an RBAC based implementation is not relevant, other access control systems can be used, such as Mandatory Access Control. [NIST AC-3 (3), (7)]
1.1.5	In support of 1.1.4, separate the duties of individuals into pre-defined roles which are documented and only the necessary privileges allocated.

Policy ID	Policy Requirement
	Where an individual has two job functions, they should be provided separate accounts from which to access the system. For example, where an individual is both a user and an administrator of a system, their user and administration privileges must be separated over two accounts. [NIST AC-5]
1.1.6	Assign access and permissions on a fine-grained basis, whereby all access to systems, applications, services and processes is denied except for those explicitly authorised for an individual's business function/role. [NIST AC-2 (i), AC-6 (4)]
1.1.7	Ensure that the access control measures of third-party or partner systems that may hold IL7 information follow this policy prior to sharing information. [NIST AC-21]

4 Procedural Requirements

Management, System Designers and Administrators shall:

Policy ID	Policy Requirement
1.1.8	Ensure that ‘entry criteria’ for all the provision of access rights to users are defined and met prior to users receiving access. Entry criteria must consider: • Acceptance of System Security Operating Procedures (SyOPs) and Acceptable Use Policy (AUP); • Justification and business need for the access; • Clearance level necessary for the access; • Training required to hold the access. [NIST AC-2c]
1.1.9	Ensure that a request and authorisation procedure for the provision of user access is generated that, prior to a user receiving access, requires: • Line or Account Manager approval; • A justification and business need for the access; • Confirmation of the user meeting the access entry criteria (as per 1.1.8); • Confirmation of user understanding and acceptance of the relevant system Security Operating Procedures (SyOPs) and Acceptable Use Policy (AUP). [NIST AC-2d, e, i]
1.1.10	Align the access management processes with IL7 or local Joiners, Movers and Leavers (JML) process such that access rights are modified or removed when: • Access is no longer required; • Users employment is terminated or transferred; • Information system usage changes. More information on JML can be found at References [6] and [7].

Policy ID	Policy Requirement
	[NIST AC-2h, PS-5(a), (b)]
1.1.11	Administration procedures are developed, in line with local/system conditions, and followed for the modification of access rights. [NIST AC-2f]
1.1.12	Periodically (at least annually, or in the event of a security incident or major non-compliance) review the quantity and justification for entity access rights and ensure that unnecessary or non-compliant access rights are removed. Where a risk assessment deems it necessary, users should be required to re-affirm their requirement to hold their access rights on a periodic basis. [NIST AC-2j, AC-2 (7a), AC-6 (7), CM-5 (5), PS-5(a), (b)]
1.1.13	Where possible, use automated mechanisms to support the management of information system access, for example using ITNow for the request, authorisation and tracking of access requests. [NIST AC-2 (1)]

5 Technical Requirements

System and Application Designers and Administrators shall:

Policy ID	Policy Requirement
1.1.14	Where possible, design systems to make use of the Privileged Account Management tooling to manage accounts and access rights to privileged functions.
1.1.15	Ensure that systems apply access control decisions upon the receipt of each request and prior to granting access to a system, service or process. [NIST AC-24]
1.1.16	Log and audit any privileged access and the execution of privileged functions. [NIST AC-6 (9)]
1.1.17	Prevent non-privileged users from executing privileged functions or executing software at higher privilege levels than the user executing the software. [NIST AC-6 (8), (10)]
1.1.18	Ensure that systems separate business functionality or user facing services from the systems management or security functionality or services. [NIST SC-2]
1.1.19	Ensure that systems notify the user, upon successful login (access) to the system, the data and time of the last login and the number of unsuccessful login attempts since the last successful login. [NIST AC-9].
1.1.20	Ensure that systems limit the number of concurrent logons to a system to one per user account. [NIST AC-10]
1.1.21	Ensure that systems will deny access to information after a period of inactivity. Systems will: • Lock the session until the user re-validates their access. • Conceal the information on the display. [NIST AC-11]
1.1.22	Ensure that systems automatically rescind access rights following a period of inactivity. This period should be defined with the CSAS Risk Assurer. [NIST AC-3 (8)]

Policy ID	Policy Requirement
1.1.23	Where possible, ensure that access to systems or services that provide security functions or access to security relevant information is denied except during secure, non-operable system states. For example, management of a firewall’s ruleset is restricted to times when no traffic is passing through it. [NIST AC-3 (5)]
1.1.24	Where a risk assessment deems it necessary, enforce access control decisions to be made on information more than identity (e.g. time of day, location etc.). For example, legitimate users may be denied access to a system outside of working hours. [NIST AC-24 (2)]
1.1.25	Where high assurance access controls are required, employ a reference monitor architecture to enforce mandatory access controls. [NIST AC-25]
1.1.26	Components that can cause a security breach if used maliciously or are accidentally compromised are identified and access to those components is strictly controlled. [NIST SC-43]

6 Privileged Access Requirements

Management and System Administrators shall:

Policy ID	Policy Requirement
1.1.27	Ensure that privileged access (including access rights associated with change) is: • Managed by a Privileged Account Management tool where possible; • Restricted to well defined roles fulfilled by nominated individuals; • Periodically reviewed to ensure that it is limited to only that which is necessary; • Not provided to individuals not employed by IL7; • Denied from or over untrusted network infrastructure. [NIST CM-5 (1), AC-6 (1), (3), (5), (6), (7)]
1.1.28	Where possible, ensure that privileged access rights are provided for a bounded period of time that is the minimum required to perform an action, after which the rights are revoked. [NIST AC-2 (6)]

7 Exemptions, Exceptions and Breaches

7.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, please refer to the exemptions and exceptions policy (Ref [8])

7.2 Breach of Policy

IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in IL7 Disciplinary Procedure.

Breaches of this Policy by a third party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third party service provider and/or the cancellation of any contract(s) between IL7 and the third party service provider.

IL7 will refer any use of its IT resources for illegal activities to the Police.