IL7
SECURITY

AUTHENTICATION POLICY

April 2020

Contents

1 Overview

IL7 Security (IL7) is committed to a layered security approach of multi-factor authentication (MFA), public/private key encryption and strong passwords whenever possible. Strong authentication remains a crucial aspect of protective security for information management systems, helping to preserve the confidentiality, integrity and availability of information by restricting access to identified users.

Conversely, poorly-designed authentication controls may result in the compromise of IL7's entire corporate system. It is therefore necessary for IL7 to impose requirements to ensure that authentication controls are implemented consistently throughout the organisation.

1.1 Purpose

Define the correct use and management of authentication controls within IL7.

1.2 Scope

This Policy applies to all systems owned by IL7, including all networks, services and applications.

1.3 Applicability

This Policy applies to all IL7 staff, service providers and contractors who use and develop systems to support IL7.

2 Authentication Policy

The following requirements will be adhered to at all times to ensure the correct use of IL7 information technology resources.

2.1 Policy and Controls

This Policy is written to ensure that the outcomes of the following Cyber Security Principles are met:

- SP-06 Operational Security (Ref [1])
- SP-07 Security Development and Configuration (Ref [2])
- SP-09 End User Devices (Ref [3])
- SP-11 Core System Protection and Separation (Ref [4])

This Policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 [5]:

AC-2	Account Management,
AC-4	Information Flow Enforcement,
AC-14	Permitted Actions without Identification,
AU-12	Audit Generation,
IA-1	Identification and Authentication Policy and Procedures,
IA-2	Identification and Authentication (Organisational Users),
IA-3	Device Identification and Authentication,
IA-4	Identifier Management,
IA-5	Authenticator Management,
IA-7	Cryptographic Module Authentication,
IA-8	Identification and Authentication (Non-organisational Users),
IA-10	Adaptive Identification and Authentication,
IA-11	Re-Authentication,
MA-4	Non-Local Maintenance,
SC-2	Application Partitioning,
SC-4	Information in Shared Resources

3 Management Responsibilities

Management responsible for security shall ensure that:

Policy ID	Policy Requirement
3.1	All users are given appropriate training and resources to allow them to comply with their authentication responsibilities, as per the Security Training and Awareness Policy (Ref [6]).

4 System Design

System designers responsible for the design of IL7 systems and the configuration of IL7 devices shall ensure that:

Policy ID	Policy Requirement
4.1	Authentication controls are used to confirm the identity of all users attempting to access IL7 resources at any time (including system-system and device-system interactions). [NIST IA-7,8,10,11, AC-2,4,14, SC-4, MA-4]
4.2	Access to systems is only granted to successfully authenticated users, in accordance with NCSC guidelines (Ref [7]). [NIST SC-2]
4.3	Multi-Factor Authentication (MFA) is implemented in line with section 5
4.4	All authentication attempts must be logged and monitored in accordance with the Logging and Log Management Policy (Ref [8]). [NIST AU-12]
4.5	All user accounts are given unique identities, in accordance with the Account Management Policy (Ref [9]). [NIST IA-2]
4.6	Username/password credentials meet the Password Policy (Ref [10]).
4.7	Authentication credentials are encrypted in transit and at rest. [NIST IA-5]
4.8	Authentication controls are reviewed as necessary when enabling/disabling user accounts during the joiners/leavers process, as outlined in the Account Management Policy (Ref [9]). [NIST IA-5]

System designers responsible for the design of IL7 systems and the configuration of IL7 devices should ensure that:

Policy ID	Policy Requirement
4.9	MFA should be utilised wherever technically possible as part of a layered security approach in accordance with NCSC guidelines (Ref [7]), alongside public/private key encryption and strong passwords as described in the Encryption Policy (Ref [11]) and Password Policy (Ref [10]) respectively.
4.10	Certificate-based authentication is considered for all situations requiring authentication.

System designers responsible for the design of IL7 systems and the configuration of IL7 devices must ensure, dependent on a risk assessment, that:

Policy ID	Policy Requirement
4.11	Any MFA implemented is appropriate to the system being deployed. Where a risk assessment deems it appropriate, in-built MFA (i.e. MFA included as part of a procured solution) should be used if available.

5 Multi-Factor Authentication

System designers responsible for the design of IL7 systems and configuration of IL7 devices shall ensure that:

Policy ID	Policy Requirement
5.1	Where MFA is used, only IL7 approved/assured MFA approaches/products are employed. Designers should contact the GRA CSAS team for information on assured products.
5.2	Where no system-appropriate IL7 approved MFA approach/product exists, the MFA solution must be assured by the GRA CSAS team.
5.3	All administrator accounts are protected by IL7-approved MFA methods. [NIST IA-2 (1, 3)].
5.4	SMS/Text Message validation is not used as the second factor. The exception to this is for citizen access to IL7 services where no other MFA mechanism is suitable.
5.5	All normal (non-privileged) user accounts that are internet facing or that utilise other public networks, including for remote access as per the Remote access design policy (Ref [12]), are protected by MFA. In this scenario, it is acceptable that the second factor is the remote access device authentication to the end system (e.g. via certificate for a VPN). [NIST IA-2]
5.6	MFA must be implemented for internal (non-administrative) user accounts, where a risk assessment deems it appropriate. [NIST IA-2]

Note: Where Multi-Factor Authentication is implemented, IL7 considers the first factor to always be a Username and Password.

6 Biometric Authentication

While biometrics can form part of a secure authentication process, the inherently probabilistic nature of the algorithms used to match the presented biometric with the information on record limits the overall level of security that can be implemented should a system rely entirely on biometrics for authentication purposes. As such additional controls should be put in place when biometrics are being considered for use to provide authentication to IL7 systems. The requirements presented here are derived from NCSC guidance (Ref [13])

System designers responsible for the design of IL7 systems and configuration of IL7 devices shall ensure that:

Policy ID	Policy Requirement
6.1	IL7 Governance, Risk and Assurance (GRA) Team support the choice of and assure any biometric systems prior to use.
6.2	Biometrics are not configured as the primary authentication method for any IL7 device – they should only be used to unlock devices to which a user has previously authenticated (such as in the case of a locked mobile phone).
6.3	Biometric data is stored “on-device” in an encrypted form and is at no point exposed outside of the device’s authentication processes.
6.4	Users are required to give consent (either on the device or separately) prior to enrolling their biometric data on a device as biometric data is, by definition, personally identifiable information under the Data Protection Act 2018 and GDPR (See references [14] and [15] respectively).

7 System Maintenance

Administrators responsible for maintenance of IL7 systems shall:

Policy ID	Policy Requirement
7.1	Abide by additional requirements for administrators laid out in the Password Policy (Ref [10]).
7.2	Ensure that remote access to any IL7 system uses valid certificates and credentials.
7.3	Not bypass authentication mechanisms for themselves or other users.

8 Exemptions, Exceptions and Breaches

8.1 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 [16]).

8.2 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.