ACCOUNT MANAGEMENT POLICY

Contents

1 No table of figures entries found.Overview

Compromised user accounts are one of the key attack vectors for hackers and hence pose a very high risk to the IL7's cyber security. Poor account management can lead to many unnecessary, un-monitored and un-managed accounts that afford malicious actors a broad attack surface from which to attack and compromise systems.

It is therefore very important to the IL7 to have strong account management processes and procedures coherent with business processes such as Joiners, Movers and Leavers, to ensure that the attack surface is minimised to that sufficient to conduct business but maintain security.

1.1 Purpose

This document defines the security requirements for Account Management that ensure that the attack surface from the compromise of user accounts is minimised.

1.2 Scope

The scope of this policy covers the managements of all accounts on IL7 systems. It does not cover access permissions and privileges which are covered under Access Control Policy.

1.3 Applicability

This policy applies to all IL7 systems and projects, including those systems delivered by third parties on behalf of the IL7.

2 Account Management Policies

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]);
- SP11 Core System Protection & Separation (Ref [2]);
- SP15 Access Control (Ref [3]).

This policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 (Ref [4]):

AC-2	Account Management
AC-3 (2)	Dual Authorisation
AC-6 (7)	Review of User Privileges

2.2 General Requirements

Policy ID	Policy Requirement
2.2.1	Understand, identify and document the numbers and types of IL7 Information system accounts necessary to conduct business and administer the relevant system. Each type of account must have an associated account manager(s) responsible for performing the managing the account of that type. [NIST AC-2a, b].
2.2.2	Ensure that accounts are only issued on a 'Least Privilege' basis whereby they only issued to those with a specific business need. To that end, it must be ensured that 'entry criteria' for all the provision of accounts to users are defined and met prior to users receiving a specific account. Entry criteria must consider: • Acceptance of System Security Operating Procedures (SyOps) and Acceptable Use Policy (AUP). • Justification and business need for the account. • Clearance level necessary for the account. • Training required to hold the account. [NIST AC-2c]
2.2.3	Ensure that a request and authorisation procedure for the provision of user accounts is generated that, prior to a user receiving an account, requires: • Line or Account Manager approval. • A justification and business need for the account. • Confirmation of the user meeting the account entry criteria (as per 2.2.2); • Confirmation of user understanding and acceptance of the relevant system SyOps and AUP. [NIST AC-2d, e, i]
2.2.4	Ensure that all issued accounts are unique and identifiable to an individual user and that accounts are not shared - with the exception of a limited number of shared accounts, see 0.

Policy ID	Policy Requirement
2.2.5	Align the account management processes with the IL7 or local Joiners, Movers and Leavers process such that account managers are notified when: • Accounts are no longer required. • Users employment is terminated or transferred. • Information system usage changes. [NIST AC-2h]
2.2.6	Ensure that administration procedures are developed, in line with local/system conditions, and followed for the creation, enablement, modification, disablement and removal from systems. [NIST AC-2f]
2.2.7	Periodically (at least annually, or in the event of a security incident or major non-compliance) review the quantity and justification for all accounts on a system and ensure that unnecessary or non-compliant accounts are removed. Where a risk assessment deems it necessary, users shall be required to re-affirm their requirement to hold a user account on a periodic basis. [NIST AC-2j, AC-6 (7)]
2.2.8	Ensure that all account creation, modification, enablement, disablement, removal and usage is logged and monitored for atypical behaviour in line with the Audit and Logging Policy (Ref [5]) and Protective Monitoring Policy (Ref [6]). Follow local security incident procedures in the event of suspicious or malicious activity. See Security Incident Management Policy (Ref [7]) [NIST AC-2g, AC-2 (4), (12)]
2.2.9	Ensure that, where possible, automated mechanisms are used to support the management of information system accounts authorisation and tracking of account requests. [NIST AC-2 (1)]

Policy ID	Policy Requirement
2.2.10	Ensure that systems: • Automatically disable user accounts after one month of inactivity. • Automatically remove or disable temporary or emergency accounts after one week of inactivity. [NIST AC-2 (2), (3)]
2.2.11	Disable suspected compromised accounts of those accounts of users that pose a significant risk to IL7, as soon as possible after the discovery of the compromise or risk. [NIST AC-2 (13)]

2.3

2.4 Privileged Accounts

Project and Programme Managers, System Designers and Administrators shall:

Policy ID	Policy Requirement
2.4.1	Ensure that stricter account entry criteria and more rigorous validation of those criteria are applied to privileged accounts. See 2.2.2.
2.4.2	Where possible, use a Privileged Account Management tool to manage Privileged Accounts.
2.4.3	Establish strict procedures for the authorisation and usage of highly privileged accounts such as Domain Administrator, or 'Break Glass' accounts. Usage of such accounts must: • Require authorisation from the Information Asset Owner or delegated individual. • Be performed by suitably trained and experienced individuals. • Use two-person controls, whereby two authorised individuals perform actions with the account and monitor each other – avoiding any potential conflict of interest. • Be recorded and audit records retained for 1 year. [NIST AC-3 (2)]
2.4.4	Ensure that Privileged accounts are different from those used for regular business. Normal business activities shall not be performed from privileged accounts.
2.4.5	Periodically (at least semi-annually, or in the event of a security incident or major non-compliance) review the quantity and justification for all accounts on a system and ensure that unnecessary or non-compliant accounts are removed. Where a risk assessment deems it necessary, privileged users shall be required to re-affirm their requirement to hold a privileged user account on a periodic basis. [NIST AC-2j, AC-6 (7)]
2.4.6	Ensure that Shared or Group accounts are explicitly monitored for atypical behaviour with priority over policy user accounts. See Protective Monitoring Policy (Ref [6])

2.5 Shared / group accounts

Project and Programme Managers, System Designers and Administrators shall:

Policy ID	Policy Requirement
2.5.1	Ensure that Shared or Group accounts are created and used by exception only. A risk assessment must be performed on all shared or group accounts, and appropriate risk mitigation measures agreed with the system Risk Assurer. [NIST AC-2 (9)]
2.5.2	Ensure that access rights to a group are terminated when a user leaves that role or group. [NIST AC-2 (10)]
2.5.3	Where possible, use a Privileged Account Management tool to manage access to Shared or Group accounts.
2.5.4	Ensure that Shared or Group accounts are explicitly monitored for atypical behaviour with priority over policy user accounts. See Protective Monitoring Policy (Ref [6])

3 Exemptions, Exceptions and Breaches

3.1 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])

3.2 Breach of Policy

The 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 the 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 the IL7 and the third-party service provider.

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