APPENDIX A. IDENTITY AND ACCESS MANAGEMENT

Category	Minimum mandatory requirements	Additional target requirements
User identification	Users accessing shared mailboxes or other resources are uniquely identified and their actions logged electronically. These are maintained for reference in the event an investigation into an anomaly or breach of policy or security is required. There are exceptions to this rule. For example, some training rooms have shared identities/passwords. In these instances, the responsible officer, such as the trainer, is to manually record which user is logged into what device to ensure that shared accounts are closely monitored to prevent and detect misuse. Other exceptions are to be treated in a similar manner. Unidentified use of resources is strictly prohibited.	
Authentication	All Department systems have automated authentication systems. However, not all are capable of complicated authentication methodology. Where technically and economically possible, the preferred methods of system authentication, in priority order, are: • multi-factor authentication (MFA); • single-factor authentication (SFA); and • password authentication.	
Multi-factor authentication (MFA)	MFA is the preferred method of authentication. MFA is required to access Department information systems and resources from a location external to the Department. Where MFA is used, a six digit PIN may be used as the secondary factor. Examples of other secondary factors include: • telephone call-back; • SMS; • security tokens; and • authenticator mobile apps. Multifactor authentication is required for access to: • critical or privileged capabilities; and • identified sensitive information.	
Single-factor authentication (SFA)	Biometric authentication is the preferred method of single-factor authentication, followed by token based authentication. Password authentication may be used as a last resort, subject to compliance with the Password System Standards (see appendix B).	

Password authentication	Where systems rely upon password authentication as their single factor, they must be configured to confirm user passwords adhere to the requirements defined in the Password System Standards (see appendix B) where technically possible. Exceptions to Password System Standards are addressed at Appendix B.	
Account locking	User accounts are locked after five unsuccessful login attempts. After that, the login screen should direct the user to contact the ICT Customer Service Centre.	Users may unlock their accounts using approved multi-factor authentication.
Suspending accounts	User accounts should be suspended: • immediately after the individual ceases work for the Department; • as directed by a responsible officer during extended periods of leave, or in case of suspension of duties; or • automatically after 90 days of inactivity.	
Protecting authentication verification information	General user: Authentication verification information cannot include passwords, passphrases, or other user credentials. Technical oversight: Authentication verification data should be stored as secure, salted cryptographically sound hashes of assigned user secret credentials and protected from unauthorised access.	
Logon banner	All systems should display a logon banner that requires the user to acknowledge and accept their security responsibilities before access to the system is granted. Logon banners should explicitly state the following conditions: • Access is restricted to authorised users only. • Acceptable usage and information security policies apply. • The user must agree to abide by the aforementioned conditions. • User activity must be monitored and audited. • Legal ramifications of violating the relevant policies. • There is no expectation of privacy when using the system (refer to Telecommunications Use Policy). • Authorised point of contact for questions on these conditions.	
Screen lock	All systems should be configured to lock the user screen and display a generic screen when locked, initiated by either: • manually locking by the user; or • after 10 minutes of inactivity. Users are required to re-authenticate to disengage the screen lock.	
Temporary access	Temporary access to information assets follow the Department's user identification requirements outlined above.	