INFORMATION AND COMMUNICATIONS TECHNOLOGY

INTRODUCTION

1.1 The Australian Defence Force Cadets (ADF Cadets) requires capable Information and Communications Technology (ICT) solutions to support the timely, effective and transparent administration of the ADFC enterprise.

POLICY INTENT

1.2 This policy outlines the minimum requirements associated with the design, provision and use of ICT systems, processes and equipment provided for ADF Cadets.

1.3 The Glossary contained in the YOUTHPOLMAN provides a list of definitions that relate to this policy.

POLICY PRINCIPLES

1.4 The principles applicable to this policy are:

1.5 Principle 1 – ADF Cadets are supported appropriately with effective ICT management and security processes.

1.6 Principle 2 – ADF Cadets ICT systems are developed, tested and sustained through a collaborative effort involving all stakeholders.

1.7 Principle 3 – ADF Cadets broadband network connections and support are fit for purpose.

1.8 Principle 4 – ADF Cadets ICT hardware assets are fit for purpose, with appropriate stocktaking processes and support.

1.9 Principle 5 – ADF Cadets web estate is managed effectively.

POLICY PRACTICES AND MEASURES

Principle 1 - ADF Cadets are supported appropriately with effective ICT management and security processes.

1.10 All information systems provided specifically for the ADF Cadets must:

a. maintain the appropriate level of security accreditation from CIOG;

b. have system documentation, including disaster recovery and system guides;

c. utilise domains approved by the Australian Government Information Management Office (AGIMO) gov.au administrators and managed through the Defence Web and Information Compliance (DWIC) team;

d. be hosted in Defence approved data centres or in cloud based providers that are on the Australian Signals Directorate (ASD) approved list; and

e. Employ contemporary industry standards for software versions and technology.

1.11 **Security**. The ADF Cadets Headquarters (ADFCHQ) is to ensure that the CadetNet information system maintains a current Chief Information Officer Group (CIOG) security accreditation at the UNCLASSIFIED (with DLM) rating. CIOG are to be advised of relevant changes to the system in accordance with the Information Security Manual (ISM) and Defence Security Manual (DSM).

1.12 **Privacy**. Privacy of information is to be in accordance with the Defence security policy which can be found at Privacy Knowledge Site.

1.13 **End user support**. Each Cadet Organisation is responsible for assigning staff to action requests for assistance from ADF Cadets members. These roles may be assigned to Australian Public Service (APS)/Australian Defence Force (ADF) or Officer of Cadets (OOC)/Instructor of Cadets (IOC) members.

1.14 **Coordination**. ADFCHQ will conduct regular meetings of ADF Cadets ICT managers and provide a report to the Joint Cadet Administrative Board (JCAB).

1.15 **Processes**. Details on procedures are located in the ADF Cadets ICT Management Protocol.

Principle 2 - ADF Cadets ICT systems are developed, tested and sustained through a collaborative effort involving all stakeholders.

1.16 CadetNet is the primary information system for the ADF Cadets and is managed by ADFCHQ, to meet the requirements of the three Cadet Organisations.

1.17 **Account Creation**. All ADF Cadets members including Defence Approved Helpers (DAH) must have an account created in the CadetNet system. Individuals who have not been formally accepted into the ADF Cadets are not to be assigned an account. Creation of AAFC accepted member's accounts are permitted until such time as the AAFC migrate member functions into CadetNet.

1.18 **Account management**. Information systems are required to have standard operating procedures maintained covering access control processes in accordance with the DSM.

1.19 **Development**. Requests for development items will be addressed through the regular meetings or relevant official project board for consideration and scheduling upon agreement.

1.20 **Sustainment**. ADFCHQ is responsible for coordinating the items included in each sustainment release which will be scheduled on a quarterly basis or as required.

1.21 **Testing**. Each Cadet Organisation will be invited to supply appropriate personnel to conduct regular testing of new modules and regression of the entire system on a routine basis.

1.22 **Processes**. Details on procedures are located in the ADF Cadets ICT Management Protocol.

Principle 3 – ADF Cadets broadband network connections and support are fit for purpose.

1.23 **Types of Connections.** Cadet units may be offered Defence funded broadband connectivity fixed connection via the National Broadband Network (NBN) or Asymmetrical Digital Subscriber Line (ADSL). Alternatively wireless mobile broadband may be provided under special circumstances. ADFCHQ has sole responsibility for the maintenance and funding of the various Defence contracts for this capability including the baseline equipment such as routers and wireless access points.

1.24 **Entitlement to a Connection**. Defence through ADFCHQ will provide a minimum of one broadband connection to each cadet organisation unit. This connection must be content filtered to ensure appropriate access for ADF Cadets

business activities only. Co-located units will share connections unless there is a business case approved by the Defence contract manager.

1.25 **Processes**. Details on procedures are located in the ADF Cadets ICT Management Protocol.

Principle 4 - ADF Cadets ICT hardware assets are fit for purpose, with appropriate stocktaking processes and support.

1.26 All Defence owned ICT hardware issued to ADF Cadets units is to be used in accordance with directives and policy issued by CIOG. This includes the initial provision/issue, nature of use, stocktake, repair, refresh and disposal through the asset's lifecycle.

1.27 **Stocktakes**. ADF Cadets must undertake and complete an ICT Asset Register stocktake in CadetNet by the notified due date for every iteration of that process.

1.28 **Refresh**. ADFCHQ coordinates refresh activity on the basis that no supported 'in service' ICT asset will be greater than 6 years of age within ADF Cadets. Costs associated with a refresh will be negotiated between CIOG, ADFCHQ and the ADF Cadets.

1.29 **Procurement**. ADF Cadets members and Defence Approved Helper (DAH) must not purchase ICT assets with Commonwealth (relevant) monies as described in the *Public Governance and Performance Accountability Act 2013*[1].

1.30 **Processes**. Details on procedures and processes are located in The ADF Cadets ICT Management Protocol.

Principle 5 - ADF Cadets web estate is managed effectively.

1.31 All ADF Cadets related web sites (both internet and intranet) must be maintained in accordance with the Defence Web Estate Manual (WEBMAN). Content must be approved by the appropriate level officer (or relevant rank / delegate) prior to being published.

1.32 **Social Media.** Policy guidance relating to ADF Cadets management and use of social media is contained in YOUTHPOLMAN Part 1.

1.33 **Processes**. Details on procedures are located in the ADF Cadets ICT Management Protocol.

RELATED POLICY

DEFENCE

Information Security Manual (ISM)

Defence Security Manual (eDSM)

Defence Web Manual (WEBMAN)

Defence Records Manual (RECMAN)

Accountable Officer: Chief Joint Capability

---

[1] http://www.finance.gov.au/resource-management/pgpa-act/

Policy Officer: Head Reserve and Youth Division