Not to be communicated to anyone outside HM Service without authority

ACSO
2190
(FIRST REVISE)

ARMY

ARMY COMMAND STANDING ORDER

NO 2190

THE SECURITY OF PERSONAL AND MISSION CRITICAL INFORMATION

ISSUED MAY 2017

Sponsored By:

Director Information

Authorised By:

Deputy Chief of the General Staff

ARMY COMMAND STANDING ORDER NO 2190
(FIRST REVISE)

THE SECURITY OF PERSONAL AND MISSION CRITICAL INFORMATION

(Army Supplementary Instructions to JSP 440 Issue 5 dated May 2014)

ACSOs in the 2000 series set out Army policy for all aspects of security. They amplify and supplement the Defence Manual of Security (JSP 440) Issue 5. Both JSP 440 and ACSOs are binding on all formations, units and establishments as defined in Paragraph 1 of LFSO 2000.

References:

A. MOD CIO Information Assurance Maturity Model (IAMM).
B. The Data Protection Act 1998 (DPA 98).
C. The Freedom of Information Act 2000 (FOIA).
D. The Human Rights Act 1998 (HRA).
E. JSP 440.
F. JSP 441.
G. Compendium of Mandated training for Unit Personnel.
H. Information Assurance Maturity Model Review Report 2016.

Introduction

1. The Army has been directed by the Cabinet Office, through the MOD Chief Information Officer (CIO) to provide assurance that Personal and Mission Critical Information Assets within the organisation are being afforded the correct level of protection, recording and management. Part of this assurance is enforceable through the Data Protection Act of 1998 (DPA 98) and supplementary direction received through the Information Assurance Maturity Model (IAMM). This ACSO serves as the Standing Order relating to the protection, recording and management of Personal and Mission Critical Information Assets within the Army.

Aim

2. The aim of this ACSO is to set out the process and procedures to be followed by all Army TLB HQs, units and personnel to afford personal and mission critical data the correct level of protection, recording and management. It provides a framework to ensure that Information Assets are assured by internal audit, and that any weaknesses are identified and rectified in order to meet the requirements of References A – G.

Application

3. This ACSO and the policy it contains applies to all Army TLB HQs, formations, units, staff branches and personnel (regulars, reserves and cadets) including those from other Services if they are part of HQs or units in the Army TLB. It also applies to:

a. Those 3rd Party Suppliers (3PS) with which the Army TLB has contracted and where the nature of the business involves the collection, storage and processing of personal data for which the MOD (Secretary of State) would be defined as the Data Controller.

b. Those Delivery Partners (DP) such as Service charities, with which the Army shares personal data.

c. Reserve Forces and Cadets Associations (RFCA) are to complete the Sid4Gov assurance program annually.

d. Cadets (ACF and CCF) are to comply with this ACSO which is the Army Policy and is articulated in the RC Cadets Branch produced Protection of Personal Information Standard Operating Procedures.

4. The ACSO does not apply to Military Museums, as these are the responsibility of Army Historical Branch. The Trustees of the museums are the Data Controllers for any personal data they hold.

Principles

5 **Information Assets.** An Information Asset can be defined as:

a. A repository of data that has value to the organisation, its business or operations and its continuity;

b. Supports a business/operational process;

c. Has longevity;

d. Is retrievable by others;

e. Is likely to harm the organisation or individual in some way (including reputational damage) if it is lost, compromised or becomes unavailable to the business;

f. Has an owner (or owners) who is (are) responsible for its through-life maintenance;

6. **Personal data.** The Army has an enduring responsibility to comply with DPA 98 and to protect and safeguard the personal information it stores and processes for all personnel (both military and civilian). Our responsibility is twofold: we must protect personal data as required by law under DPA 98; and we must ensure that personal data does not fall into the hands of those who may wish to exploit it.

7. Personal information is defined as[1]: 'Data which relate to a living individual who can be identified:

a. From those data, or

b. From those data and other information which is in the possession of, or is likely to come into possession of, the Data Controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'[2].

8. **Mission critical information.** A Mission Critical Information Asset is defined as: Information that is indispensable to delivering the day-to-day running, mission or operational capability of any unit, formation or establishment. This should not be confused with the Unit/Establishment Security Officer's 'Unit Asset Register' that records the types and quantities of assets that the unit is responsible for protecting. MOD CIO has directed at Reference H the need to afford protection to our mission (or 'business') critical information.

Management of Information Assets

9. In order to provide the correct level of assurance to our information assets the Army has developed the Army Information Asset Register (AIAR). Formation HQs across the TLB and their

[1] DPA 98, Part 1. 1(1) (e).
[2] The Data Controller is the Secretary of State for Defence.

subordinate units that hold positions within the AF8005 Establishment Table are mandated to use the AIAR to record the following data:

a. Personal information assets.

b. Mission critical information assets.

c. Risk assessments and Privacy Impact Assessments (PrIA).

d. Exemption certificates.

e. Storage and processing of assets and the systems in use.

f. IT Security Accreditation of systems in use.

g. Personnel assigned to mandated protection/information governance roles and their training.

h. Personnel assigned to all security roles and their training.

i. A record of training achieved for unit personnel (Defence Information Management Passport (DIMP), Responsible for Information or the Protecting Information Level 0 Presentation that can be included at end of MATT6).

10. **Assurance.** Internal audit processes provide important assurance that the processes and procedures directed in this document are being followed and legal and mandatory requirements are being met. The following two groups will meet in support of these objectives:

a. **The Information Assurance Delivery Group (IADG).** Terms of reference for the IADG are at Annex D, Appendix 1. Members will be required to use the tools made available to them[3] to provide regular assurance of compliance within their area of responsibility (AOR).

b. **The Third Party Supplier Information Assurance Group (3PS IAG).** Terms of Reference for the 3PS IAG are at Annex D, Appendix 2.

11. **Subject Access Requests[4].** The Army HQ Data Protection Support Team (DPST) will provide the focal point for policy and guidance with regard to Subject Access Requests (SARs) made to the Information Commissioner's Office (ICO) or received directly by HQs or units. Accordingly, the DPST will not routinely handle SARs or redact information for disclosure. In the first instance, SARs are to be submitted to the unit or establishment Data Protection Officer (DPO) who is to ensure that it is forwarded to the appropriate body for action. This may be the unit or establishment receiving the SAR or another organisation within the Army TLB or the MOD.

12. **Detailed instructions.** Due to the breadth and detail required in the management of information assets Annexes A to D provide the detailed instructions for those concerned with both personal and mission critical information.

Summary

13. Correct management of our personal and mission critical information is key to understanding what data we hold on our personnel and what mission critical assets we are relying on to provide training and generate capability in order to deliver our outputs. Protecting and managing these

[3] Army Information Asset Register (AIAR) on-board reports.
[4] Full guidance on how to progress a SAR can be found at: Army Data Protection Website/Subject Access Requests.

vital assets is everyone's business and the AIAR, coupled with the policy and guidance in this ACSO, will provide the Chain of Command (CoC) with the assurance that this is happening.

D Info

Annexes:

A. Army Data Protection Policy.
B. Registration and Management of Information Assets.
C. Unit Information Team Functional Construct.
D. Terms of Reference for the Groups and Individuals.
E. Breach Management Plan.

ARMY DATA PROTECTION POLICY

References:

A. Data Protection Act 1998 (DPA 98).
B. JSP 440 – The Defence Manual of Security.
C. LFSO 2008 – Communication & Information Systems (CIS) Security.
D. JSP 441 Managing Information in Defence.

Introduction

1. The Army needs to collect and use certain types of personal data for the purposes of satisfying business, operational and legal obligations. The Army recognises the importance of the correct and lawful treatment of personal data and the need for all personnel (regardless of their role) to recognise their individual responsibility to handle and protect personal information in order to meet the requirements of DPA 98.

2. The Army fully endorses and adheres to the 8 principles of the Data Protection Act. All personnel (Military, Civilian, RFCA including ACF & CCF, 3PS and Delivery Partners (DP)) who obtain, handle, process, transport and store personal information for the Army must adhere to these principles.

Principles

3. As defined in DPA 98, personal data is: 'Data which relates to a living individual who can be identified; from that data, or from that data and other information which is the possession of, or is likely to come into the possession of, the Data Controller[5] and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

4. There are 8 principles of DPA 98 which must be followed when obtaining, storing, processing and disposing of personal data[6]. The principles require that personal data shall:

a. Principle 1: Be processed fairly and lawfully and shall not be processed unless certain conditions are meet;

b. Principle 2: Be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner that is incompatible with the original purpose;

c. Principle 3: Be adequate, relevant and not excessive for those purposes;

d. Principle 4: Be accurate and, where necessary, kept up to date;

e. Principle 5: Not to be kept for longer than is necessary for that purpose;

f. Principle 6: Be processed in accordance with the data subject's rights;

[5] The Data Controller is the Secretary of State for Defence. For the purposes of this ACSO, the data controller will be taken to mean the Army acting on behalf of the Ministry of Defence.
[6] Subject to the provision of exemptions at Appendix 2.

g. Principle 7: Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using appropriate technical and organisational measures;

h. Principle 8: Not be transferred to a country or territory outside the European Economic Area, unless there are adequate levels of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

5. Guidance on the application of these principles is contained in Appendix 1.

Rights of the Individual

6. All individuals who are the subject of personal data held by the Army are entitled to be informed of the following information:

a. The identity of the data controller.

b. The identity of any representative of the data controller.

c. The purpose(s) for which their data are intended to be processed.

d. Any further information which is necessary to enable the processing in respect of the data subject to be fair[7].

Subject Access[8]

7. All individuals who are the subject of personal data held by the Army are entitled to[9]:

a. Be given by the data controller a description of the personal data of which they are the data subject.

b. Be told the purposes for which their personal data is being (or will be) processed.

c. Be provided with details of recipients, or classes of recipients, to whom their data may be disclosed.

d. To have communicated to them in intelligible form the information constituting their personal data.

e. Any information available regarding the source of their data.

8. The Army will make every effort to ensure that the data subject receives this information within 40 calendar days of making their request in accordance with DPA 98[10].

Data Security

9. The Army recognises the need to ensure that personal data is kept secure during all aspects of processing in accordance with DPA 98, Principle 7. Personnel are to take all necessary steps

[7] 'Fairness' is not defined by DPA 98, however, some of the things that breach the 8 principles are clearly defined as 'unfair'. Some examples of information that should be included to ensure processing is fair are: information on outsourcing or the use of Data Processors/Contractors; disclosures to third parties; additional information on the Data Subject's rights and anything else that is relevant to ensure transparency.
[8] DPA 98, Section 7(1), (a-d).
[9] Subject to the provision of exemptions at Appendix 2.
[10] Certain responsibilities apply to responding to a subject access request (eg verifying the identity of the individual). Guidance is available on the Army Data Protection website.

against physical loss or damage, unauthorised access and unauthorised disclosure. To this end, all personnel are responsible for ensuring that:

a. Any personal data for which they are responsible is kept securely in accordance with References B and C.

b. Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

c. Personal information is not accessed by any unauthorised personnel.

Retention of Data

10. The Army will retain some forms of personal information for longer than others. All Information Asset Owners are responsible for insuring that the information they are responsible for is not kept longer than necessary for the purpose for which it was obtained, in accordance with DPA 98, Principle 5 and in accordance with Reference D[11].

Areas of Responsibility

11. The key data protection governance roles are outlined at Annex C. Terms of reference for the Information Assurance roles are at Annex D.

12. All personnel (regardless of role) are responsible for:

a. Ensuring their mandated data/information handling training is current.

b. Checking that any information that they provide to, or on behalf of, the Army is accurate and up to date.

c. Understanding the Government Security Classification (GSC) system and handling personal data appropriately, in accordance with legislation and MOD/Army policy.

Supporting Material

13. This policy is to be read in conjunction with MOD Information Rights Compliance Team data protection guidance notes[12] and Army guidance and direction that is published on the Army Data Protection Website[13].

Appendices:

1. The 8 Data Protection Principles – overview.
2. Exemptions.

[11] JSP 441 – Part 2, Guide, Records 05, Annex A Appendix 2
[12] MOD Information Rights Compliance Team Guidance Notes
[13] Army Data Protection Website

Appendix 1 to
Annex A to
ACSO 2190
Dated May 17

DATA PROTECTION ACT 1998 – THE 8 PRINCIPLES

1. The DPA is an enduring legal requirement.

2. The Act covers not only computerised data, but also manual records held in a structured (or 'relevant') filing system[14] and is designed to safeguard individuals from the harm or embarrassment that could be caused by the loss or unauthorised disclosure of their personal information. It regulates the holding and processing of information relating to living individuals and gives them legally enforceable rights. In addition, it places legal obligations on those persons who control and process personal data.

3. Within the Army we hold and process vast quantities of personal data. We must protect the personal data to comply with the law – compliance is not optional.

4. The intention of the Act is not to prevent the processing of personal information, but to ensure it is done fairly and lawfully. To this end, DPA 98 is underpinned by a set of 8 principles which incorporate the 'essence' of the Act and can be used as a guide. All Army personnel are individually responsible for ensuring that any personal information processed or held (whether about Service or Civilian personnel, or members of the public) is handled in accordance with the eight principles. In summary, these principles are as follows:

The 8 Principles of DPA 98

DPA 98 Principles	What does this mean?
1. Personal data must be fairly and lawfully processed.	'Processed' means collecting, storing, retrieving, and holding, using, structuring, filing and destroying personal data. You should have legitimate grounds for collecting and using the personal data and be transparent about how you intend to use it. You should handle people's personal data only in ways they would reasonable expect you to. If you do not have clear consent from the data subject(s) to process their data you must seek advice on whether you can lawfully do so.
2. Personal data must be processed for limited purposes.	Be clear from the outset about why you are collecting personal data and what you intend to do with it. When personal data is collected it can only be used for the purpose(s) for which it was obtained and should not be used for another, incompatible, purpose.
3. Personal data must be adequate, relevant and not excessive.	The personal data you hold should only be sufficient to carry out the purpose for which it has been collected. It must also be relevant to that purpose. Make sure that you do not hold more information than you need – if it is not required, why is it held?

[14] This includes all handwritten notes and notebooks.

4. Personal data must be accurate and up to date.	You are responsible for ensuring that the personal data you manage is accurate and up-to-date. Inaccurate information can lead to wrong decisions being made to the detriment of the data subject(s). Ensure that there is a procedure in place (and utilised) for keeping your information up-to-date.
5. Personal data must not be kept for longer than is necessary.	It is unlawful to keep personal data for longer than is necessary. Doing so increases the risk that data will be out of date and that it may be compromised. If information is no longer used, ensure it is properly archived, deleted or destroyed[15]. Point to note: There are bans on destruction of material related to – NI, Iraq, Afghanistan and the Goddard Inquiry[16]
6. Personal data must be processed in line with the data subjects' rights.	An individual has the right to request information about them which is held by the MOD, this includes personal opinions. This is known as a Subject Access Request (SAR). An individual has the right to prevent processing which is likely to cause damage or distress. This is hard to prove. An individual has the right to prevent processing for purposes of direct marketing. Within an RHQ, each option should be an Opt In, ie Email, Newsletter, SMS. An individual has the right to challenge any decision which has been made solely by automated means for the purpose of evaluating matters, ie performance at work, grants. An individual has the right to compensation if they have suffered damage and distress. This however is very difficult to prove in a court. If an individual's data is inaccurate, they have the right to request the MOD to rectify (excluding medical records where a note will be added), block, erase or destroy. Depending on the information requested by an individual there might be an exemption which is applicable to certain areas and should be taken into account. Exemptions can be found at Appendix 2.
7. Personal data must be secure.	Only people who are authorised to process the information should have access to it. It should be sufficiently protected physically (locked away); procedurally (permissions and internal controls) and electronically (passwords or encryption).

[15] Destruction of Protectively Marked Information – JSP 440, Part 4, Section 2, Chapter 1.
[16] Disposing of Records – JSP 441 Part 1, Para 50

	Data can easily be accidentally disclosed if it is left on an unattended desk or computer screen, if it is overheard in a conversation or found in a bin! Large amounts of personal data can be held on small devices – for example, it is possible to lose thousands of records on a memory stick that can fall out of someone's pocket!
8. Personal data must not be transferred to other countries without adequate protection.	Sometimes personal data is processed outside of the UK. All personnel must be aware of the risk when they are dealing with processing personal data outside of the UK. A Memorandum of Understanding (MOU) or Data Sharing Agreement will be required if you are dealing with any country outside of the European Economic Area[17]. For International Exercises, within Army TLB there is an International Agreements Branch which can give help and advice in relationship to MOUs. Defence has an MOU database which records all MOUs between Head Office and other nations and organisations.[18] Permanent Overseas MOD locations, ie BGN or BATUK, are considered as being UK territory for the purposes of the DPA.

Information covered by the DPA 98

5. DPA 98 covers information that is:

   a. Processed by means of equipment (eg a computer);

   b. Part of a 'Relevant Filing System':

      A set of information relating to individuals which are manual records and are structured either by reference to individuals or be reference to criteria relating to individuals in such a way that is readily accessible, ie handwritten notes & notebooks.

   c. Part of an 'Accessible Record':

      A health record, an educational record or an accessible public record.

   d. For example:

      (1) Paper Files ('P-Files').

      (2) Electronic Files, Databases, Spreadsheets and Emails.

      (3) Photographs (including CCTV footage, Pass Photo databases etc).

      (4) Publications.

[17] The European Economic Area (EEA) is the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market.
[18] Defence MOU Database

(5) Web Pages.

Note: This is not an exhaustive list.

DATA PROTECTION ACT 1998 – EXEMPTIONS

1. The rights and duties set out in the Data Protection Act are designed to apply generally, but there are some exemptions from the Act to accommodate special circumstances.

2. If an exemption applies, then (depending on the circumstances) you will be exempt from the requirement:

a. to grant subject access to personal data; and or

b. to give privacy notices; and or

c. not to disclose personal data to third parties

3. Depending on why you are processing personal data, you may be able to use an exemption. You must consider each exemption on a case-by-case basis.

4. Several specific exemptions are set out in Part 4 and Schedule 7 of DPA98.

a. Preliminary.

b. National security.

c. Crime and taxation.

d. Health, education and social work.

e. Regulatory activity.

f. Journalism, literature and art.

g. Research, history and statistics.

h. Manual data held by public authorities.

i. Information available to the public by or under enactment.

j. Disclosures required by law or made in connection with legal proceedings etc.

k. Parliamentary privilege.

l. Domestic purposes.

m. Miscellaneous exemptions.

n. Powers to make further exemptions by order.

o. Transitional relief.

REGISTRATION AND MANAGEMENT OF INFORMATION ASSETS

References:

A. DPA 98.
B. JSP 440.
C. JSP 747.
D. Information Assurance Maturity Review Report 2016

Introduction

1. Information is a key business asset and its correct handling is vital to the delivery of our services and the management of our personnel. In striking the right balance between sharing and protecting information, we must continually manage business impacts and risks associated with the confidentially, integrity and availability of our information. To this end, ownership, at an appropriate level, of all Information Assets containing personal information was mandated across the TLB in Dec 08. The same level of visibility and ownership was extended to mission critical assets following direction from MOD Chief Information Officer (CIO) in Reference D.

2. Several policy initiatives have been put in place across the MOD over the last few years as principles to determine and assess the seriousness of the risks to the business, or harm or distress to individuals, should a compromising event occur, and to allow priority to be given to tackling those situations where risk is most likely to materialise. These are detailed below.

Governance Structure

3. D Info heads the Army Information Assurance (IA)/DPA network in his capacity as the Army's Senior Information Risk Owner (SIRO). The SIRO is supported by the Head of Cyber & Security, who is the Senior Data Protection Officer (SDPO). Hd Cyber & Sy delegates authority to manage the Army's IA responsibilities to AH CI & Sy as the Head of the CI & Security in Army HQ and the Army TLB Principal Security Advisor (PSyA). Within that branch, the principle staff officer in respect of IA/DPA is SO1 IA[19] who is supported by the Army Data Protection Support team and a network of Data Protection Officers/Information Asset Owners across the TLB.

4. At unit level, COs/Heads of Establishment (HoE) are to appoint a Data Protection Officer (DPO), although this role may be combined with other duties. In many units the Regimental Administrative Officer (RAO) would be best placed to be the DPO, given their expertise in handling personal data on a daily basis. The generic Job Description for RAOs includes a reference to the DPO role and it is shown on the unit organisation diagram at Annex C.

5. In support of the above, an internal audit process is in place to provide assurance of compliance and clarify areas of responsibility. This is underpinned by two working groups:

a. The Information Assurance Delivery Group (IADG), incorporating formation level representation from all appropriate areas, which meets quarterly.

b. The Third Party Supplier Information Assurance Group (3PS IAG), a quarterly meeting attended by Subject Matter Experts (SME) from the Army Commercial, Information Security and Data Protection fields.

[19] Email: Army Info-CyberSy-IA-SO1.

6. Commanders/Leaders/Managers at all levels must ensure that their staff are appropriately trained and that they apply IA/DPA principles and practices properly. They must act as role models and set examples of good practice.

7. In order to make sure that the Army is DPA 98/Policy compliant, a robust Governance Structure is in place throughout the TLB. The unit level roles and associated functions are outlined in the diagram at Annex C. These functions and outputs are mandatory.

8. The terms of reference for the key governance roles are at Annex D.

Identification, Ownership and Registration of Information Assets

9. The Army is required by the MOD CIO to maintain a register of the totality of its holdings of information assets. The Army Information Asset Register (AIAR) has been developed and its use is mandated throughout the TLB to meet this requirement. The AIAR holds a comprehensive list of all personal and mission critical information assets held by the Army and provides a profile of the type of information within the asset, principle storage method, format, usage and likely impact on the business should a compromising event occur.

10. The AIAR also records the details of the individual who is responsible for each registered asset, the Information Asset Owner (IAO) and the IA/DPA governance role holders for any given unit. The AIAR provides an auditable record of all personal and mission critical information assets which have been identified and registered to date and is managed by the Army Data Protection Support Team (ADPST - a part of the larger Army HQ Information Assurance Team).

11. Identification and ownership of personal and mission critical information assets at an appropriate level within the TLB is mandatory. The IAO for an Information Asset will be the individual who is best placed to control the information, has access to it and is responsible for:

a. The 'day-to-day' safe use of the Information Asset, including the setting of permissions.

b. Confirming the continuing need to hold the information.

c. Registration of the asset with the AIAR.

d. Maintenance of the AIAR registration record (minimum every 3 months).

e. Ensuring that any personal information within an Information Asset is handled within the 8 principles of the DPA 98 and in accordance with MOD and Army policy and directives.

12. Guidance on identifying a Personal Information Asset is at Appendix 2. Guidance on identifying a Mission Critical Information Asset is at Appendix 3.

13. When an information asset is created that contains, or may in the future contain, personal data, there will be a need for a Privacy Impact Assessment (PrIA) to be produced[20]. Depending on the category and quantity of the data[21] one of the following will need to be produced:

a. A full scale Privacy Impact Assessment or

b. A Data Protection Self-Assessment or

c. An Exemption Certificate.

[20] 2010DIN05-065 gives more details on Privacy Impact Assessments.
[21] Appendix 2 gives details of types of personal data and volume thresholds.

The IAO is responsible for producing the PrIA and getting it approved; A PrIA template can be downloaded from the AIAR. Once produced, the PrIA is to be uploaded and recorded on the AIAR.

14. IAOs must account for any printed electronic records of the same information in which they are not the AO and must be identified as a new asset, (ie JPA reports) as the risks of compromise and means of controlling access are different. Personnel are strongly advised to reduce to an absolute minimum the duplication of information assets containing personal data as this only increases the likelihood of a Data Protection Breach, not just because of unauthorised access but also the versions containing different data; this would potentially breach Principle 4 of DPA 98 – data held must be accurate and up to date.

Training

15. Completion of an appropriate level of data handling training is an enduring MOD mandatory[22] requirement. All personnel (both Service and civilian) are required to undertake training at a level commensurate to their role and to ensure it is refreshed at appropriate intervals.

16. Guidance on the training required for staff is in the matrix at Appendix 1. All units will be required to report compliance statistics annually through the AIAR to Army HQ in support of SIRO's annual reports to MOD CIO. In order to support this requirement, HQs and units are advised to collate their training statistics using a locally produced spreadsheet[23] although, in time, it is hoped to be able to use the competences functionality on JPA and HRMS.

17. In order to assist the audit of training, units should keep the paper copies (or some other record such as a scanned copy) of certificates issued to individual on completion of the mandatory training. These records are to be kept for the period that the certificate is valid, which is currently 3 years for DIMP and 3 years for RFI (either General user or IAO or SIRO). Absence of a record at inspection or audit will be treated as evidence of non-completion of training.

Assurance and Oversight Activity

18. Oversight of compliance is provided by the DPST in Army Info CI & Security Branch.

19. All personnel (including contractors) working with Army information assets have a collective responsibility to ensure that information is protected from compromise, misuse and illegal or malicious activity. Within the TLB, key standards (at Appendix 4) have been provided by the IA team to be used by DPA/IA governance role holders during inspection and review to assess compliance and provide a common framework for analysis. The standards have been incorporated into reports within the AIAR and reflected in the Unit Administration Manual (UAM) Part 8, i-Admin Questions for consistency.

20. The assurance functions that have been associated with the key standards to ensure that IA/DP compliance is at an acceptable level and that any weaknesses are identified and rectified by prompt action are:

a. Oversight of all Information Assets via registration with the AIAR.

b. Oversight of the risk management of assets (via the AIAR).

c. Local level management (conducted at unit level by the Unit Personal Information Risk Manager (PIRM) and Data Protection Officer (DPO) using the AIAR 'on-board' reports).

d. Audit (G1Audit - unit level).

[22] 2015DIN07-139
[23] Training Courses Template

e. Audit (By the DPST - at Army HQ).

f. Regular review (via management information provided to the IADG).

g. Self-assurance.

21. Periodic assurance of compliance with DPA 98 and the policy in this ACSO is conducted in one of 3 ways:

a. The G1 Audit. Many units are subject to formal inspection by the G1Audit team and this audit includes questions relating to the protection of personal data and mission critical information.

b. Audit by the Army DPST. Some 1* and 2* HQs, mainly in Army HQ, are formally audited by the Army DPST, which will issue a report to the relevant HQ.

c. Any HQ or unit not formally audited by the G1Audit team or the Army DSPT is to conduct a self-assurance assessment at least annually, using the UAM Part 8 Question set[24]. The outcome of this self-assurance is to be reported to the DPST via the AIAR using the tab 'View Assets'. Once the self-assurance has been completed, the DPO should use the calendar and record the date completed within Initial Audit date. The grading the unit receives will determine the date by which the unit will need to review and conduct self-assurance again. This will be recorded using the calendar in the Audit Review date. If a grade of Green or Yellow is received, the next review will be in 2 years; for a grading of Amber or Red a review will need to be completed after 6 months.

Collectively, these provide a robust data protection assurance framework that covers the TLB.

Electronic Filing, MOSS and Meridio

22. A very large amount of personal data and mission critical information is stored electronically, currently on MOSS and Meridio for DII users. MOSS and Meridio provide functionality to limit access to sensitive information to those entitled to see it. HQs and units are, therefore, to ensure that appropriate information is stored in limited access MOSS and Meridio sites and that staff are informed which sites to use, and how to get access if they need it.

23. It is vital that the relevant permissions on limited access sites are set up correctly and regularly checked. This not only prevents unauthorised users accessing the sites directly, it also prevents anyone searching for data being shown the results of searches to sites where they do not have access. It is important to note that file permissions in Meridio do not transfer automatically to Meridio; they must be set separately.

24. Anecdotal evidence suggests that the most likely time that limited areas are discovered to have been opened to all users is following a MOSS upgrade. Therefore, units are to ensure that limited areas are checked to ensure they are appropriately secure; the easiest way to do this is to employ a 'buddy' system with another iHub who do not normally have permissions to view your limited areas. Correctly limited areas are not normally visible unless the user has permissions to this area and so if areas that obviously should be limited can be seen then permissions will need to be reset.

Communications

25. A diagram showing the command chain for the downward flow of information from Army HQ regarding IA/DPA issues is at Appendix 5.

[24] UAM Chapter 8 Question set

26. Any queries regarding this directive are to be directed to the Army HQ DPST or Divisional/Formation IADG representative in the first instance.

Appendices:

1. Information Management and Data Handling Training Requirement.
2. Assets containing Personal Information.
3. Assets containing Mission Critical Information.
4. Key Standards.
5. IA/DPA Chain of Command Diagram.

Appendix 1 to
Annex B to
ACSO 2190
Dated May 17

INFORMATION MANAGEMENT AND DATA HANDLING TRAINING REQUIREMENT (AS AT 1 JUNE 2016)

Training Course	Requirement
Defence Information Management Passport (DIMP) (including the Government Security Classification (GSC) scheme and Responsible for Information (General User)) *(DLE Cse Code: INFO MATTERS)*	**Mandated 3 yearly:** To be completed by all Service Personnel, Civil Servants and Contractors who manage and handle information and who regularly access Defence Information Systems. New entrants to MOD/Armed Forces are to complete this training within 3 months.
Responsible for Information (General User) *(DLE Cse Code: RFI_GU)*	**Mandated 3 yearly:** To be completed by all Service Personnel and Civil Servants who manage and handle information but **do not** regularly access Defence Information Systems. New entrants to MOD/Armed Forces who fall within this category are to complete this training within 3 months. **The approved Army TLB alternative to this course is Protecting Information Level 0 which is also mandated 3 yearly**.
Responsible for Information **(Information Asset Owner) or (Senior Information Risk Owner) or (Non-Executive Director and Boards)** *(DLE Cse Codes: RFI_IAO, RFI_NEDS, RFI_SIRO)*	**Mandated 3 yearly:** To be completed by all Service Personnel, Civil Servants and Contractors who manage and handle information, have regular access to Defence Information Systems and are employed as Information Asset Owners, Senior Information Risk Owners and Non-Executive Directors and Board Members. Training is to be completed commensurate with the role and within 3 months of taking up the post.
Data Protection Overview *(DLE Cse Code: DP Overview)*	**Mandated once** for all Data Protection Officers within 3 months of taking up their role.
Army HQ Data Protection Workshop *(Bookings can be made via this Link)*	**Recommended once** for Data Protection Officers and Data Protection Governance role holders.

Notes:

- **Defence Information Management Passport** (DIMP) v4 is a new course which replaces the old Information Matters (IM) Passport and incorporates the RFI General User course. All regular DII users must complete the DIMP once their IM Passport or RFI General User course expires. Users whose most recent Data Protection training is Protecting Information Level 1 must complete the DIMP as soon as possible.
- **Protecting Information Level 1** has expired and is no longer valid.
- **Protecting Information Level 0** Links to **Protecting Information Level 0 Presentation** and **Protection Information Level 0 Facilitator Notes**. Requests for a copy on CD for use on non DII IT can be submitted to the Army Data Protection Support Team (ADPST). CDs will be issued to units/organisations whose personnel do not have access to DII.

- **Responsible for Information** (RFI) training suite is available on CD from the ADPST for those who do not have access to DII. This CD can only be used on non-DII IT (eg standalone computers) and is designed for use by units/organisations whose personnel do not have access to DII.
- **Data Protection Workshop** is a practical one-day workshop providing education on the Governance Structure, Training, and Principles of the Data Protection Act, as well as a briefing on Personal Information Assets, Privacy Impact Assessments and the Assurance Regime. The workshop also provides an insight into the Army Information Asset Register (AIAR).
- Other MOD Mandated Training can be found at this Link

ADPST can be contacted via '<u>Army Info-CyberSy-DPA-0Mailbox (MULTIUSER)</u>'

ASSETS CONTAINING PERSONAL INFORMATION

1. **Information.** An information asset is a collection of information that is:

   a. A repository of data that has value to the organisation, its business or operations and its continuity;

   b. Supports a business/operational process;

   c. Has longevity;

   d. Is retrievable by others;

   e. Is likely to harm the organisation or individual in some way (including reputational damage) if it is lost, compromised or becomes unavailable to the business;

   f. Has an owner (or owners) who is (are) responsible for its through-life maintenance;

2. **Definition.** A collection of personal information records is referred to as a Personal Information Asset (PIA) and can be defined as:

   a. Any holding of any quantity of records of personal data, in any format, such as paper or electronic, from which an individual can be identified.

3. **Identification.** Personal information can range from the benign (a simple record of name and telephone number) to sensitive information requiring a minimum protective marking of OFFICIAL-SENSITIVE PERSONAL (such as a criminal conviction), or a combination of both. Asset owners in conjunction with the PIRM are required to determine which category their information falls into and whether it qualifies for registration with the AIAR.

4. **Examples.** The table on page B2-2, though not exhaustive, provides a ready guide, with examples and the level of protection required. In addition to the data types listed in column 1, there may be a case where the aggregation of these records requires re-classification to OFFICIAL-SENSITIVE PERSONAL[25]. For example, a database, electronic folder, storage device or paper based filing system containing 1000 or more records of this type would ordinarily be re-classified as OFFICIAL-SENSITIVE PERSONAL.

5. **Site Access Management System (SAMS).** These are used to issue passes to staff and visitors; the most common package used by the Army is SYSIS. These will inevitably hold large volumes of personal data. As such they must be handled accordingly, ie recorded on the AIAR, a full PrIA completed and appropriate documentation for the use of the application must be completed. Common themes we have encountered are:

   a. No data retention policy for the system on the site – Principle 4.

   b. Identifying the correct IAO, a person who understands and knows the business, ie Site/Unit Security Officer.

   c. Are the free text boxes being used appropriately, taking into account an individual may request all information held on them – Principle 6

[25] 2010DIN02-009 (this DIN has not yet been updated with the correct classifications).

Any specific SAMS questions can be addressed to SO1 IA – 94393 6805.

One or more of the following pieces of information which can be used to identify an individual:		Information about that individual the release of which is likely to cause harm or distress:	
CAT A • Name • Work/Business Address • Work/Business Email • Postcode • Telephone numbers • Date of birth • Service/Staff Number • Identifiable Photograph **These records alone amount to 'Business Card' details and WILL NOT require registration via AIAR** **HOWEVER** **Do you hold large volumes of this data type?** **If the number of records exceeds 1000, it may warrant 'OFFICIAL SENSITIVE PERSONAL' status depending on the nature of the individuals, source of the information, quantity and extent of the information and will require registration with the AIAR.** **ASSESS AND MANAGE THE RISK**	**COMBINED WITH[26]**	CAT B • Pay, banking or financial details • National Insurance Number • Passport Number • Driving license number[27] • Performance Reporting (MS) details (OJAR/SJAR/PADR) • Next of Kin (NOK)/Family Details (spouse/partner/children) • Home address • Home email • Medical Information (Blood Group) • Record of Service • Education/Qualification Details • Welfare information, such as material relating to social services/ child protection/housing • Tax, benefit or pension records • DNA or fingerprints CAT C • Sexual/gender matters • Physical or mental health condition • Religious beliefs or other beliefs of a similar nature • Political opinions • Racial or ethnic origin of the data subject • The commission or alleged commission of any offence • Any casework or record relating to any offence committed or alleged to have been committed, AGAI 67 proceedings and the disposal of such proceedings or the sentence of any court. • Membership of a trade union (within the meaning of Trade Union and Labour Relations 1992) • Free Text Boxes	REQUIRES A MINIMUM PROTECTIVE MARKING OF **'OFFICIAL-SENSITIVE PERSONAL'** **These records require registration with AIAR**

[26] eg, one or more pieces of information which can be used with public domain information to identify an individual combined with information about that individual whose release is likely to cause harm or distress.
[27] Note that driving license number is included in this list because it directly yields the first part of the surname and date of birth.

Registration of PIA with the AIAR

6. All PIA that meet one or more of the following criteria must be registered with the AIAR and assessed for DPA 98 compliance:

a. The asset contains 1000 records or more of CAT A;

b. The asset contains less than 1000 CAT A but also includes CAT B;

c. The asset contains CAT C personal information as defined by DPA 98;

d. The asset is sometimes transferred outside the unit, department or organisation;

7. All PIA containing over 1000 records must be registered with the AIAR[28] by the PIAO. However, the 1000-record threshold is to be used as a guide only. It is likely that there are many PIAs in use with less than 1000 records which should be registered with the AIAR. This is because of the nature of the personal information they hold (for example, sensitive personal information). If the impact of an unauthorised person misusing the information would be high, the PIRM and PIAO must assess the risk and may choose to register the asset irrespective of the quantity of records.

8. If a PIA only contains public domain or 'business card' information (such as name, work telephone number and work email address) it does not need to be registered with the AIAR unless the number of records exceeds 1000. However, if it contains public domain or 'business card' information and also links it to other information about the individuals, so that, once combined it becomes quite powerful by association and/or potentially damaging to the individuals, then it must be registered. For example:

a. A unit telephone list contains the name, rank, branch and work telephone number of unit personnel and does not exceed 1000 records. It does not need to be registered with the AIAR.

b. A unit telephone list contains the above information, but also links the names to a SF unit, particular exercise or other sensitive (or private) information. By association the asset will now present a much higher risk should a compromising event occur and the assessed Business Impact Level is likely to be higher. Therefore, the asset should be registered with the AIAR.

[28] Note: PIAs that are held on an accredited MOD system such as DII(F) will have to be registered with the AIAR if they meet the criteria above.

ASSETS CONTAINING MISSION CRITICAL INFORMATION

1. **Definition.** Mission Critical Information (MCI) is defined as Mission, Training, Business Task, Finance or Output Critical Information that is indispensable to delivering the Running, Mission, Operational Capability or Outputs of the Unit, Formation or Establishment. This is not to be confused with the Unit/Establishment Security Officers Unit Asset Register from LFSO 2011 that will record the type and quantity of material that is classified.

2. **Identification.** The decision on whether information is classed as MCI can only reside at the unit, formation or establishment that holds and uses it. In order to decide whether a piece of information is Mission Critical the overarching question is 'Can we do our job, our mission, our operation or operate without this information?'. If the answer is 'no' then the item is Mission Critical and must be recorded in the Army Information Asset Register (AIAR). MCI can be soft or hardcopy, files, folders or MOSS sites and range from Instructional Specifications within a Training Regiment to Op Orders at a Formation HQ. The following are the types of information that could be considered as MCI:

   a. Documentation in the form of Op Orders, FRAGOs etc that are key to the running of the unit or establishment or any contingency operation the unit or establishment may be involved in.

   b. Current, but not historical unit generated Op Orders.

   c. Locally produced and maintained matrices outside of ODR.

   d. Equipment sustainability/serviceability states created outside of MJDI and JAMES.

   e. Within a training regiment this could well be the ISPECS for training from which lesson plans could be reproduced if all else was lost.

Information that is entered in centrally held databases such as MJDI, ODR, Blenheim etc is managed at the highest level and need not be recorded at unit or formations level.

3. **Registration.** All information that is considered as MCI by units, formations and establishments is to be recorded on the AIAR in a similar manner to the recording of personal information assets. The process of recording allows the asset owner to undertake an element of Information Risk Management and this allows Army HQ to interrogate the AIAR and understand where a risk to information is being carried.

4. **Combined Assets.** There may be occasions when MCI contain personal data, in which case these assets are to be afforded the same protection as personal data assets as detailed in Appendix 2. Combined Assets are to be recorded as such on the AIAR.

5. **Examples.** Representative information is given in the table overleaf and should be used as a guide to entering information into the AIAR.

Mission Critical Information – Examples

For the analysis of and registering of Mission Critical Information Assets.

Asset and Custodian	Details (held in/on, location and handling process	PM Qty	Impact (I) of loss, compromise or mis-management (High (5), Med (3) Low (1))	Vulnerability issues LIKELIHOOD (L) (High (5), Med (3) Low (1))	Risk Score			Comments (How to manage the risk)
					I	L	Total	
Paper; Bn Op Order, Op Programme, PORs and Operational Int updates, CO 3 Regt	Paper, held in Secure cabinet in Ops Office, accounting for using MOD 102 processes.	Secret 33	Risk – OPSEC Impact – High (5) – Compromise of Operational Information and Programmes and Op Int. Threat to unit personnel and Theatre.	Low (1)	5	1	5	Continue to conduct MOD102 accounting processes.
Paper; Trg matrix and Deployment Transport Plan (RIP) CO 3 Regt	Paper, held in Secure cabinet in RAO office, accounted for using local processes.	Official Sensitive 150	Risk – OPSEC & PERSEC Impact – Med (3) – Compromise and Threat to personnel in trg locations or during move to Theatre	Med (3)	3	3	9	Conduct more frequent accounting checks using Duty Officer
Electronic; Current Op Battle Rhythm and Operational Int updates CO 3 Regt	Electronic, held on DII(F) Secret UAD, HDD is stored in machine during working hours (manned) and in Secure cabinet in Ops office out of hours	Secret 150, growing by 10 per week	Risk – OPSEC Impact – High (5) – Compromise of Operational Information and Programmes and Op Int. Threat to unit personnel and Theatre.	Med (3)	5	3	15	Continue to conduct MOD102 accounting processes
Electronic; Pre-Op planning emails. CO 3 Regt /10 Armd Bde	Electronic, held on DII(F) Restricted UAD. HDD is stored in UAD permanently. UAD is in secure Ops Office.	Official Sensitive 1000+ growing by 100 per week	Risk – OPSEC & PERSEC Impact – Med (3) – Compromise and Threat to personnel in training locations or during move to Theatre.	Med (3)	3	3	9	Continue to conduct out of hours guard checks on building security
Electronic; ISPECS Trg Wing	Electronic files held on DII(F) Restricted MOSS site	Official 56	Risk – Loss of Training Impact – High (5) Unable to conduct training on unit specific equipments	Low (1)	5	1	5	Ensure hard copy is produced and updated in line with electronic files.

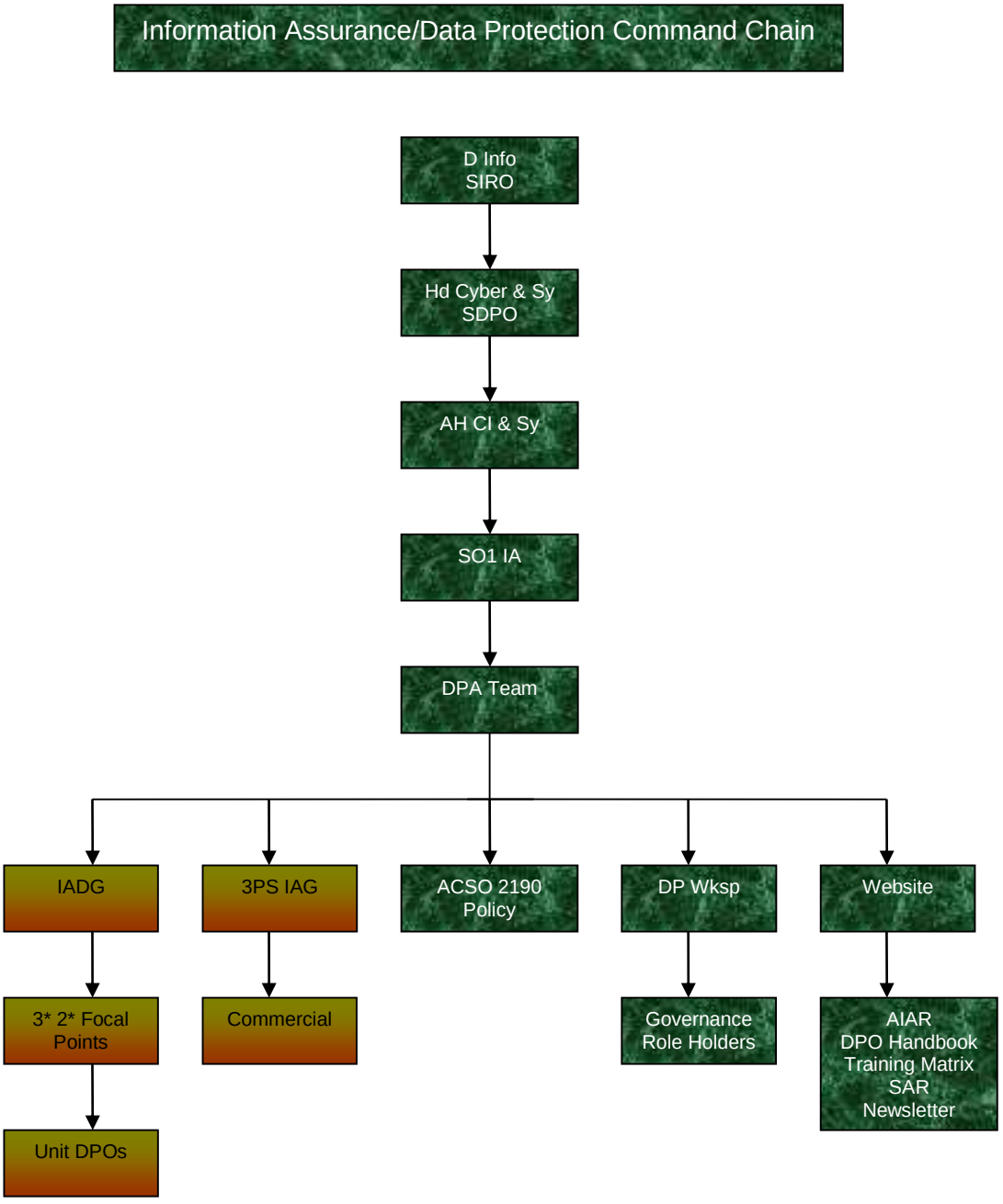
Appendix 4 to
Annex B to
ACSO 2190
Dated May 17

KEY STANDARDS

Serial	Key Standards
1	The IA/DPA Governance Framework has been implemented and all key roles are populated.
2	A current, signed EUN[38] Certificate of Conformity is on file.
3	The Information Risk Owner is kept informed of how much (personal information) risk the unit has.
4	Information is addressed as a standing agenda item at all suitable management level meetings and boards.
5	All Governance Role Holders have been given guidance on how DPA 98 relates to their role, understand the specific responsibilities placed upon them and are properly equipped to meet mandatory data protection requirements.
6	An educational awareness programme is evident (to include publication of the Data Protection Officer's (DPOs) contact details).
7	Information Risk Awareness has been built into all staff inductions.
8	All personnel (including contractors) have received Information Risk Awareness training at a level appropriate for their role (the unit must be able to provide up to date evidence of compliance and annual refresher training).
9	All Information Assets have been identified and registered with the Army Information Asset Register (AIAR).
10	Information Asset Owners have been identified for each Information Asset.
11	Information Asset Owners have a system in place to routinely undertake a quarterly review of their PIAs.
12	Information Asset Owners have either conducted a Privacy Impact Assessment, a Data Protection Self-Assessment or an Exemption Certificate for their information asset within the last twelve months (LFSO 2008 refers).
13	Information Risk Managers understand the vulnerability and likelihood of loss/compromise of the Information Asset from various threats.
14	Information Asset Owners and Information Risk Managers have used Business Impact Levels to make a balanced assessment of the countermeasures to meet risk management requirements for confidentiality, integrity and availability of their (Personal) Information Assets.
15	Information Asset Owners and Information Risk Managers have used Likelihood level assessments and assigned a proportionate level of protection to mitigate, and/or recover from, the potential loss of their Information Assets.
16	Access to Information Assets is correctly managed and safeguarded throughout the lifecycle of the Information Asset (ie access is granted only to those who have a business requirement and appropriate security clearance).
17	Proper application of the Government Security Classification System is in evidence for all Information Assets.
18	Proper physical security of Information Assets has been addressed (ie storage of protectively marked material – especially assets containing sensitive personal data or large quantities of personal data).
19	Information Asset Owners are aware of, and have implemented, corrected data retention and weeding protocols for their asset.
20	Staff are aware of the correct protocols for reporting an information/data protection breach.

[38] The Electronic Unit Name (EUN) is used as a unique unit identifier.

IA/DP Internal Communications Command Chain



Annex C to
ACSO 2190
Dated May 17

UNIT INFORMATION TEAM FUNCTIONAL CONSTRUCT

Red = Security Roles/Linkage
Purple = IM Roles
Green = DPA & MCI Roles
Orange = Crypto Role

Responsibilities:
1. **Senior Risk Owner (SRO)** as per ACSO 2011 (inc responsibility for Information & Personal Information Risk) for their AOR. Ultimately responsible via CofC to D Info as SIRO & SSRM.
2. Also holds the role of **Senior Information Owner (SIO)** and **Information Asset Owner (IAO)** for Business Critical (defined as being Official to TS and critical to the units outputs) Information Assets
.

Unit/Branch CO or HOE
(Lt Col to 1)*

Responsibilities:
1.Is the Unit Risk Manager (has day to day responsibility for Risk Management (inc. Business Critical & Personal Information Assets) and owns Risk Register as per LFSO 2011).
2. Security Advisor (as **USO or ESyO**) and Info Assurance lead.
3. See notes 4, 5, 9 and 11.

2I/C or COS
Depending on Unit, Fmation or Garrison/ Station (SO1 or SO2)

PVRO
See Note 13

Crypto Custodian
(See 12)

Info Manager (IMgr)
(SO2 or SO3)
See Notes 9 & 11

Is the Info Risk Manager.

IT Security Officer
(SO2 to SNCO)
See Notes 4, 5, 7, 9 & 10

Data Protection Officer
(SO2 or SO3)
See Note 6 & 9

Info Support Officer *(RAOWO)*

I-Hub Functions:

Information Support Assistants
Records Management (inc. F102)
Team Site Admin (MOSS)
DII/F Authorised Demander (AD)
Defence Intranet Manager
Guaranteed Point of Access (GPOA)
Local registration Authority (LRA) for PKI

Resources will be variable in terms of Nos, military, civil servant.

(See Notes 1, 2, 3 & 7)

DII/F Local Security Officer (LSO)
See Notes 3 & 7

CIS Platoon / G6 Staffs

BITSOs, Sub Unit ITSOs
(1 per sub unit or remote location)
See Notes 8,9 & 10

System Managers & Admins
(TLANs, Laptops, Standalones, Internet Pcs etc)

Data Protection Assistant(s) (DPA)
Det Command or RAOWO
See note 6, 8 & 9

Core I-Hub

Approved Users of Unit Systems *(Stand alones, UWO, Internet systems etc)*

Personal Info Asset Owners

Info Asset Owners (for Mission Critical Information)

USERS

Rules/Assumptions:
1. The main system will be DII/F/MODnet
2. I-Hub has many functions but most are secondary roles with normal user turnover.
3. The AD, LRA and LSO are mandated DII/F roles; mandated separation of AD & LSO.
4. USO & ITSO must be separate individuals.
5. Units will need to ensure double coverage of mandated posts for deployment, ie deploying & rear party.
6. DPO is the appointment/person whose core business is to identify personal and mission critical information assets are registered and properly managed.
7. ITSO & LSO could be the same appointment/person – there is some functional linkage.
8. BITSO & DPAs are delegated sub unit as/if required (typically for dispersed sub units)
9. Functions can be delegated depending on resources, training and experience.
10. DITSO/ITSO trained staff are authorised to provide cascade training to BITSOs.
11. FOI is routine CofC business.
12. Crypto Custodian role governed by JSP 490/491.
13. PVRO training is provided by SMIT/214MI.

Glossary

Authorised Demander (**AD**) –Responsible for submitting Service Requests (New users, new UADS, password updates, software downloads etc) on behalf of a Business Unit. Should be more than 1 per unit.
Branch Information Technology Security Officer (BITSO) - In larger or widely separated establishments such as formation HQs or Reserve units, a BITSO is required to assist the Information Technology Security Officer (ITSO) (see below).
Crypto Custodian – A JSP 490 mandated role responsible for the safe custody, registration, mustering, amendment, issue, safe handling and disposal of cryptographic items held by a Business Unit or at a location. This duty is to be delegated to an individual who is responsible to the CO or HoE.
Data Protection Officer (DPO) - EUN-level lead for implementing DPA 98, typically the RAO within a unit. Focus of effort will be the 8 DPA Principles and ensuring Personal Information Asset Owners and all PIA users are aware of their data handling responsibilities.
Data Protection Assistant (DPA) – Individuals with delegated responsibility, from the DPO, for DPA 98 issues with in a sub unit or remote element of the EUN.
Defence Intranet Manager (Army Intranet Publisher) - Management of web content in unit and formation including publishing of information on the Defence Intranet.
Establishment Security Officer (ESyO) – Mandated role responsible for implementing and monitoring MOD and TLB Security Policy, esp. physical and guarding, and acts as Security Advisor to the CO/HoE.
Guaranteed Point of Contact (GPoC) - All official information should be sent to Group Mailboxes. The GPoC ensures that Official information is received and dispatched through the unit First sight System iaw a unit's battle rhythm.
Information Asset Owner (IAO) - Anyone responsible for the creation, maintenance, utilization and distribution of MOD owned data that contributes to the running and outputs of a Business Unit.
Information Hub (iHub) - The focus for all Information Administration (iAdmin) at unit level, and underpins effective Information Management. The iHub's task is to ensure the effective receipt, storage, distribution, archiving and disposal of information.
Information Manager (IMgr) - Accountable for the information process in the organisation. The IMgr advises and supports the Senior Information Officer (SIO) and is responsible for ensuring that information is being captured, stored, distributed, used, retained, and eventually disposed of, in accordance with MOD policy.
Information Support Assistant (ISA) - Work in the iHub and are responsible to the ISO for Information Administration activities.
Information Support Officer (ISO) - Head of the iHub, and responsible for the good management and exploitation of information within the organisation.
Information Technology Security Officer (ITSO) – JSP 440 & LFSO 2008 mandated role, appointed by ESyO who is responsible for overseeing the implementation of and adherence to CIS Policy in a Business Unit.

Local Security Officer (LSO) – Responsible for some aspects of DII Security in a Business Unit and the interface with ATLAS on security matters.
Personnel Information Asset Owner (PIAO) – Anyone responsible for the collection, maintenance and use of personal data held in a Personal Information Asset (PIA).
Personal Information Risk Manager (PIRM) - Responsible for managing the risk of all Personal Information Assets (PIA) held within their organisation. Maintains the risk register of all PIAs and advices the PIRO on the risk held.
Personal Information Risk Owner (PIRO) – Is accountable for the identification and registration of all Personal Information Assets (PIAs) held within the organisation.
Personnel Vetting Records Officer (PVRO) – Responsible for maintaining the Business Units Register of current staff vetting and managing vetting clearances on behalf of the CO/HoE.
Senior Data Protection Officer (SDPO) – HD IS is responsible for ensuring that personal information is processed, across the Command, in accordance with DPA 98, subsequent and emerging Departmental guidance, JSP 440 and JSP 441.
Senior Information Officer (SIO) – Responsible for all aspects of Information Risk within the organisation with a specific remit to enforce security and assurance of all data held. Normally this is a senior officer reporting directly to the CO/HoE.
Senior Information Risk Owner for the Army (Army SIRO) – D Info is the Army SIRO. He reports to CGS and advises Defence SIRO on information matters affecting the Army.
System Administrator – A role delegated by the System manager with responsibility for the day to day management and control of a system.
System Manager – Is responsible for the management and operation of a system to the System Owner, in this instance the CO or HoE.
Team Site Admin (TSA) – Responsible for setting up, maintaining and monitoring Business Unit MOSS sites and access to them.

TERMS OF REFERENCE

1. In order to make sure that the Army is IA/DPA compliant, a robust governance structure is in place throughout the TLB. The governance structure is outlined in Annex B and in the diagram at Annex C. These are functions and outputs that must be delivered.

2. The Terms of Reference (TORs) for the IA/DPA governance roles are at the following Appendices:

a. Appendix 1 – Information Assurance Delivery Group (IADG).

b. Appendix 2 – Third Party Supplier Information Assurance Group (3PS IAG).

c. Appendix 3 – CO/Commander/Head of Establishment – Personal Information Risk Owner (PIRO).

d. Appendix 4 – COS/2IC – Personal Information Risk Manager (PIRM).

e. Appendix 5 – Data Protection Officer (DPO).

f. Appendix 6 – Personal Information Asset Owner (PIAO).

g. Appendix 7 – Information Asset Owner (IAO).

h. Appendix 8 – Third Party Supplier (3PS).

i. Appendix 9 – Delivery Partner (DP).

Information Assurance Delivery Group (IADG)

Purpose

1. To deliver Information Assurance, including data protection policy and governance, in accordance with legislation and MOD/Army policy as part of the Army Operating Model and the Army's overarching Information sub-strategy.

Role

2. Members are to work with the Army Headquarters Information Assurance Team to promote the Army Information Assurance and Data Protection agenda within their area of responsibility.

Frequency

3. The Information Assurance Delivery Group will meet quarterly.

Responsibility

4. The Information Assurance Delivery Working Group will:

   a. Promote and advise on legislation and MOD/Army policy, rules and guidance.

   b. Promote and advise on the Army Information Assurance/Data Protection Governance Framework.

   c. Advise Commanders at all levels of training requirements and promote educational awareness and staff training initiatives that support the cultural change plan in raising awareness throughout the Army.

   d. Monitor compliance with the governance framework and drive action to improve compliance in parts of the TLB that are weak.

Responsibilities and Tasks of the Information Assurance Delivery Group Members

5. In addition to the collective tasks detailed above, the Information Assurance Delivery Group members will:

   a. Identify and where possible, manage the key issues that could impact on the delivery of Army Information Assurance and Data Protection policy in their area of responsibility.

   b. Act as the Information Assurance/Data Protection focal point for their area of responsibility.

   c. Identify and report risks to delivery in their area of responsibility.

   d. Encourage, monitor and evaluate activity within their area of responsibility.

   e. Encourage Information Assurance (including Data Protection) to be addressed as a standing agenda item on all Executive Boards and Audit Committees.

f. Share best practice with other group members.

g. Submit a quarterly report on data protection compliance within their area of responsibility to the Information Assurance Delivery Group.

Membership

Chair: SO1 IA

Army HQ Staff Officer Leads: SO1 IA, SO2 Data Protection,

Members: 3 and 2 Star level Information Assurance/Data Protection focal points.

Secretary: SO3 DPA (Governance).

Third Party Supplier Information Assurance Group

Purpose

1. To establish and maintain a constructive dialogue between Subject Matter Experts (SMEs) in the fields of Information Assurance, Data Protection and Commercial Services in order to provide assurance that effective information risk management is being applied to Army Third Party Suppliers (3PS).

Role

2. Members are to work with Army Headquarters Information Assurance Team to promote the Army Information Assurance 3PS agenda in accordance with legislation and MOD policy.

Frequency

3. The Third Party Supplier Information Assurance Group (3PS IAG) will meet bi-annually.

Responsibilities of the 3PS IAG

4. The 3PS IAG will:

   a. Utilise the management information from the SID4GOV tool to drive 3PS assurance on behalf of the TLB;

   b. Identify and manage areas of risk;

   c. Identify barriers and accelerators for secure data handling in respect of 3PS;

   d. Provide visibility of due diligence;

Responsibilities of 3PS IAG Members

5. In addition to the collective tasks detailed above, the 3PS IAG members will:

   a. Act as the information assurance focal point for their subject matter area;

   b. Oversee an annual assurance cycle;

   c. Identify and report risks to delivery in their area of responsibility;

   d. Where possible, manage the key risks that could impact on the delivery of assurance with regard to Army 3PS;

   e. Share best practice with other group members;

   f. Input to the end of year summary report to inform SIRO’s annual report to MOD CIO.

Membership

Joint Chair: SO1 IA
Comrcl Army HQ PCAT C1

Members: SME Leads: Comrcl Trg Mgr, SO2 DPA, Comrcl Army HQ PCAT E1.

Secretary: SO3 DPA (Assurance)

CO/Commander/Head of Establishment – Personal Information Risk Owner (PIRO)

1. The CO/Comd/Head of Establishment (HoE) is the unit/HQ PIRO. They are ultimately responsible for all aspects of organisational risk relating to information assets which contain personal or mission critical information, with a specific remit to enforce compliance with DPA 98 and the relevant policies associated with security and assurance of information held within their Area of Responsibility (AOR).

2. The PIRO shall champion best practice within the unit/HQ in order to support the Army strategic objective of transforming the way we manage, share, present and exploit information to deliver Information Superiority (IS), whilst ensuring compliance with relevant legislation.

3. The PIRO is required to ensure that all key governance roles are established within their AOR and for ensuring that data protection is addressed as a standing agenda item at a suitable management level meeting in accordance with Key Standard 4.

4. The PIRO is accountable, through the CoC, to the Army's Senior Data Protection Officer (Hd Cyber & Security) for the identification and registration of all information assets on the AIAR which contain personal or mission critical information and which are held within their organisation.

5. The PIRO is to sign a EUN Certificate of Conformity[30] at least once annually (or when a new incumbent takes up the post) to confirm that their unit is either compliant or to record areas of non-compliance and actions or mitigations that are in place. This action is in support of Army HQ's requirement to submit a consolidated annual SIRO report to Defence SIRO (Chief Digital and Information Officer; CDIO).

[30] EUN Certificate of Conformity example.

COS/2IC – Personal Information Risk Manager (PIRM)

1. The PIRM is responsible for the unit level information risk management. Specific responsibilities are:

a. Ensuring best Information Security practice within the unit/HQ are encouraged, are reported on and re-educating as appropriate where personnel are found to be failing in their IS duties.

b. Ensuring all Personal and Mission Critical Information Assets within the unit have been identified, protected, handled, shared and stored in accordance with their classification and that they are appropriately owned and registered with the AIAR.

c. Overseeing and directing the granting of AIAR access permissions by the DPO, who is the unit/HQ lead for managing permissions.

d. Completing a Risk Assessment with the Information Asset Owner for each of the organisation's personal or Mission Critical Information Assets, assessing the probability and impact of any compromise of the data held therein using Business Impact Levels[31].

e. Overseeing a bi-annual review of information assets within the unit to ensure that the AIAR listing is maintained in an up-to-date state.

f. Ensuring all new arrivals receive an awareness brief on DPA principles, their legal rights and responsibilities regarding personal data and the need to register Personal and Mission Critical Information Assets if owned/created. This should be incorporated into extant induction programmes.

g. Providing a Certificate of Conformity, which details the risk that a unit is holding when required as part of the IA/DPA compliance audit routine.

h. Providing the PIRO with a regular report of the information assets for which he is responsible, providing an overview of any areas of non-compliance an action plan.

i. Creating and drafting the EUN Certificate of Conformity using the AIAR functionality provided. Ensuring that this is presented to the PIRO annually, for his/her signature, highlighting all risk.

j. Leading investigations into suspected or alleged breaches of DPA 98 and/or MOD/Army policy, informing the CO/HoE (as PIRO) of the investigations findings and then implementing any lessons identified in order to prevent a reoccurrence.

[31] Business Impact Levels (BILs) were introduced in around 2008/09 but were removed from JSP 440 with the introduction of the GSC as the two systems did not tally up. However legacy CESG IA Standards still refer to BILs, and they may be used in Accreditation, as does the extant 2010DIN02-009 on DPA. The Army Data Protection Team has decided, therefore, to retain the use of BILs in the AIAR and DPA Documentation for continuity purposes. This will be reviewed with future changes in CESG IA documentation and changes to MOD Policy

Local Data Protection Officer (DPO)

1. The DPO is the unit focal point for all IA/DPA matters. Specific responsibilities are:

a. Promoting Information Assurance and Data Protection awareness within the EUN.

b. In conjunction with the PIRM, identifying all holdings of personal and mission critical data throughout your organisation and ensuring all Information Assets are registered with the AIAR.

c. In liaison with the PIRM, ensuring the appointment of Information Asset Owners for each of the personal and mission critical information assets identified and providing guidance and support to the information asset owners.

d. Acting as the unit lead for granting AIAR access permissions to the Information Asset Owners. (Note that the PIRM will also have permissions for granting access).

e. Collating the EUN Memorandum of Understanding (MOU) database.

f. Managing a quarterly review mechanism in the organisation to ensure that Information Asset Owners periodically review their Information Assets. The review should query the following:

(1) The purpose(s) for which personal/mission critical data are being processed;

(2) That the data are adequate and relevant for the purpose(s) and not excessive;

(3) That the data are as accurate and up-to-date as necessary for the purpose(s);

(4) That a data retention policy is in place and applied for each Information Asset data type.

(5) A comprehensive risk assessment has been recorded for each asset.

g. Delivering the day-to-day work required to enable the IAO's compliance with their responsibilities and, to this end, undertaking monthly 'housekeeping' using the AIAR 'on-board' reports to ensure that the unit maintains a satisfactory level of compliance.

h. Timely and accurate recording of any data losses in accordance with extant procedures. Reporting must include whether the data was registered with the AIAR.

i. Keeping the PIRM informed of any significant risks posed to Information Assets held by the EUN.

j. Ensuring any multi-user Information Assets are registered only once with the AIAR and have only one Information Asset Owner. Ownership should be assumed at the highest level of the asset.

k. Maintaining a training record for all personnel within their unit to ensure the appropriate level of training is completed at induction or within 3 months of taking up post and refreshed

when required, reporting compliance statistics to Army HQ via the AIAR as directed. Additional individual training records are to be maintained for the following roles:

(1) Personal Information Risk Managers (PIRM).

(2) Data Protection Officers (DPO).

(3) Data Protection Assistant (DPA)

(4) Personal Information Asset Owners (PIAO).

(5) Information Asset Owners (IAO).

(6) Establishment/Unit and Branch Security Officers (ESyO/USO/BSyO).

(7) DII Local Security Officer (LSO).

(8) Establishment/Unit and Branch IT Security Officers (ITSO/BITSO).

l. Providing a conduit for advice on DPA 98 rather than being a DPA expert ensuring specialist or complex DPA issues are referred to the Army Data Protection Support Team (ADPST).

m. Acting as a Focal point within the unit for all Subject Asset Requests (SARs).

n. Supporting the PIRM in investigating any suspected or alleged breaches of DPA 98 and/or MOD/Army policy.

2. The DPO is not responsible for:

a. Providing an expert assessment of whether each Information Asset is used ‘safely’.

b. Completing and maintaining the asset records on behalf of the Information Asset Owners or for keeping their training compliance details up to date.

c. Being the HQ’s/unit’s authoritative source of DPA compliance information.

Personal Information Asset Owner (PIAO)

1. The PIAO is responsible for the day-to-day 'safe' use of their Personal Information Asset by completing the following actions:

a. Confirm the continued need to hold personal data record(s) from which individuals could be identified - thus qualifying it as a 'Personal Information Asset'.

b. The asset must be maintained in accordance with the 8 DPA Principles. A Full Privacy Impact Assessment or a Self-Assessment must be produced and maintained in accordance with 2010DIN05-065[32] to provide assurance that a thorough assessment against the 8 Principles has been completed for each Personal Information Asset.

c. Maintaining an up-to-date registration report of their Personal Information Asset by:

(1) Ensuring each Personal Information Asset is registered electronically via the AIAR.

(2) Providing the DPO with regular assurance that all of their Personal Information Assets are assessed and registered as requested.

(3) Updating unit logs of any subject access requests and disclosures made and all regular data sharing agreements which are in place for the asset.

d. Complete a periodic review of the Personal Information Asset in order to keep the AIAR up-to-date, to know that your asset is still relevant and current to the business. This should be carried out every 3 months[33] or when any of the following occur:

(1) Any significant change to the content or records stored;

(2) The Personal Information Asset is no longer to be used and is deleted or archived;

(3) A change in purpose of the processing of the Personal Information Asset;

(4) The access arrangements to the personal information significantly alter;

(5) A change of PIAO.

And should include the following:

(6) A check to ensure that the list of 'data items' is up-to-date.

(7) Maintenance of an up-to-date Full Privacy Impact Assessment, a Self-Assessment to provide assurance that a thorough assessment against the 8 Principles has been completed for each Personal Information Asset.

(8) A review of the recorded Business Impact Level to ensure it is still appropriate.

[32] 2010DIN05-065
[33] 2010DIN02-009 Annex C refers

(9) A review of access controls.

(10) A review of document retention periods.

(11) Addressing any risks to their Personal Information Asset.

(12) Ensuring that the movement of information onto removable media has been minimised and all removable media associated with the asset are accounted for.

Note: The date of completion of each review is to be noted in the appropriate field of the AIAR and will be taken as an electronic signature by the PIAO that all risk management elements and checks are up to date for audit purposes.

2. The PIAO is not responsible for:

a. Being the authoritative source of DPA compliance information. They should be able to refer any enquiries to the DPO due to the complex nature of the legislation.

b. Training individuals in the correct application of the DPA.

3. In addition to maintaining their information assets, PIAOs are responsible for updating their training compliance on the AIAR.

Information Asset Owner (IAO)

1. The IAO is responsible for the day-to-day 'safe' use of their Information Asset by completing the following actions:

a. Confirm the continued need to hold the Mission Critical Information Asset.

b. The asset must be maintained in accordance with Army Policy[34] to provide assurance that a thorough assessment has been completed for each Mission Critical Information Asset.

c. Maintaining an up-to-date registration report of their Mission Critical Information Asset by:

(1) Ensuring each Mission Critical Information Asset is registered electronically via the AIAR.

(2) Providing the DPO with regular assurance that all of their Mission Critical Information Assets are assessed and registered as requested.

(3) Updating unit logs of any disclosures made and all regular data sharing agreements which are in place for the asset.

d. Complete a periodic review of the Mission Critical Information Asset in order to keep the AIAR up-to-date, to know that your asset is still relevant and current to the business. This should be carried out every 3 months[35] or when any of the following occur:

(1) Any significant change to the content or records stored;

(2) The Mission Critical Information Asset is no longer to be used and is deleted or archived;

(3) A change in purpose of the processing of the Mission Critical Information Asset;

(4) The access arrangements to the information significantly alter;

(5) A change of IAO.

And should include the following:

(6) A check to ensure that the list of 'data items' is up-to-date.

(7) Maintenance of an up-to-date Exemption Certificate to provide assurance that a thorough assessment has been completed for each Mission Critical Information Asset.

(8) A review of the recorded Business Impact Level to ensure it is still appropriate.

(9) A review of access controls.

(10) A review of document retention periods.

[34] ACSO 2190
[35] 2010DIN02-009 Annex C refers

(11) Addressing any risks to their Mission Critical Information Asset.

(12) Ensuring that the movement of information onto removable media has been minimised and all removable media associated with the asset are accounted for.

Note: The date of completion of each review is to be noted in the appropriate field of the AIAR and will be taken as an electronic signature by the IAO that all risk management elements and checks are up to date for audit purposes.

2. The IAO is not responsible for:

a. Being the authoritative source of DPA compliance information. They should be able to refer any enquiries to the DPO due to the complex nature of the legislation.

b. Training individuals in the correct application of the DPA.

3. In addition to maintaining their Mission Critical Information Assets, IAOs are responsible for updating their training compliance on the AIAR.

Third Party Suppliers (3PS)

1. The definition of a 3PS is a company or organisation that has an established contract with the Army TLB which is established through Commercial Branch.

2. All commercial contracts must include a DEFCON 532A/B or a framework substitute relating to Data Protection Policy.

   a. DEFCON 532A – Protection of Data (Where personal data is not being processed on behalf of the authority)

   b. DEFCON 532B – Protection of Data (Where personal data is being processed on behalf of the authority) which places obligations on the contractor and the MOD to handle Personal Data in accordance with DPA98.

3. Contractors must complete the Sid4Gov assurance program annually upon request from SO3b Data Protection.

4. Any issues flagged through Sid4Gov should be reviewed by the contractor and actioned accordingly within the designated timeframe stated on the report.

5. All breaches of Data Protection must be reported to the Army Warning Advice Reporting Point (WARP) as per the Army Breach Management Plan at Annex E.

Delivery Partner (DP)

1. A Delivery Partner is an MOD term for an organisation with which the MOD conducts regular data exchanges in support of mutual aims but has not entered into a contract with.

2. All Delivery Partners should either have an extant Memorandum of Understanding (MOU)[36] or Service Level Agreement (SLA) with the Army TLB stating the agreed mutual relationship and the respective obligations of each party taking into account their data processing and storage of personal data. Examples of Delivery Partners in the Service charitable sector would be Help for Heroes, SSAFA and Army Benevolent Fund.

3. The fair and lawful processing requirements for DPA Principle 1 will need to be considered in respect of any proposed data sharing by looking at Schedules 1 & 2 of the Act. The necessity for a Data Sharing Agreement should be considered for each case.

4. All MOUs in relation to personal data should be notified to the Army Data Protection Team[37].

5. All breaches of Data Protection must be reported to the Army Warning Advice Reporting Point (WARP) as per the Army Breach Management Plan at Annex E.

[36] MOU Template
[37] MOU Spreadsheet

BREACH MANAGEMENT PLAN

General

1. The purpose of the Army Data Protection Breach Management Plan (DP BMP) is to ensure a standardised approach across the Army in the reporting, containment and management of a breach[38] involving personal data throughout the management of an incident by Army Warning Advice and Reporting Point (WARP). Army 3rd Party Suppliers (3PS) and Delivery Partners are also to report a Data Protection Breach to Army WARP so that they can receive an appropriate level of assistance[39].

2. A breach, loss or compromise of personal data may be the result of either:

   a. Loss or theft of equipment or storage (ie cabinet) on which data is stored;

   b. Inappropriate or inadequate access controls allowing unauthorised use;

   c. Human error;

   d. Unauthorised disclosure;

   e. Accidental destruction;

   f. Hacking or targeted attack;

   g. Unforeseen circumstances such as fire/flood.

Control

3. Data Protection Breach Management is the business of the Personal Information Risk Manager (PIRM), Data Protection Officer (DPO), Personal Information Asset Owner (PIAO), Unit Security Officer (USO) and IT Security Officer (ITSO). In the event of a breach (actual or suspected), unit data protection and security staff are to:

   a. Appoint an Incident Manager to coordinate the unit/organisation response to an incident and manage actions until the incident is closed.

   b. Identify all stakeholders, for example higher formation SECURITY staff within the CoC, Adjutant etc.

   c. Review Annex A to determine precisely what elements of personal data have been breached, lost or compromised.

   d. Delegate activities and form understanding of the circumstances leading to the incident to inform the initial, IMMEDIATE unit/organisation report to Army WARP.

4. The Incident Manager is to complete the data protection breach management summary action table (see Appendix 2), recording a **summary** of actions taken until the incident is closed.

[38] A breach could include loss and/or compromise of personal data.
[39] 3PS and Delivery Partners can inform Army WARP via ArmyWARP-Mailbox@mod.uk

The Summary Action Table is an auditable record and is to be retained by the unit/organisation for 2 years.

Action

5. The Incident Manager is to coordinate the below activities and be assisted by unit security and data protection staff in the management of a Data Protection Breach. It is important to take IMMEDIATE action to help reduce harm and distress to data subjects and limit the potential for reputational damage to the Department. It is also important for Army Headquarters to identify trends and improve policy, processes and procedures to avoid recurrence. Activities are as follows:

a. **Immediate Report to Army WARP.** A breach, loss or compromise of personal data, no matter how small in scale, is to be reported to Army WARP[40] IMMEDIATELY, by the Incident Manager, using MOD Security Incident Response Scheme Submission Form (eMSF)[41]; a link & guidance can be found on the Army WARP intranet site. The Army WARP will then generate an Incident Number and initiate an investigation (if necessary), commensurate with and proportional to, the level of risk and nature/scope of the incident. The eMSF is to contain as much information as is known at the time of reporting and must not be delayed to facilitate the inclusion of additional information that could be provided at a later date. Immediate reporting will provide early notification to the CoC, facilitate compliance with onward reporting times and allow timely counter compromise and remediation action to be taken.

b. **Containment and Recovery.** A data protection breach will require not just an initial response, but also containment and recovery including where necessary, damage limitation. It is important to establish quickly whether there is anything that can be done to recover any losses and limit the scope of further damage the breach has or could cause. Unit data protection and security staff may require input from across the business area or specialist advice from Army WARP or the Data Protection Support Team (DPST). The Incident Manager is to establish who needs to be involved in containment and recovery and inform them of their activities to achieve it. Activities could include isolating or closing social media sites, initiating a search for lost equipment or documents or changing access codes to a secure cabinet or office. The Incident Manager is to complete the Damage Assessment Report and submit to Army WARP[42] as soon as possible after initial containment and recovery action.

c. **Assess Risk to Data Subjects and MOD Reputation.** The Incident Manager is to be assisted by unit data protection and security staff in assessing the risk to data subjects and the department's reputation resulting from the breach; a unit case conference may be necessary to achieve this. If additional information about the circumstances and scope of the breach is received, the initial assessment of risk may need to be reviewed and further action taken; for example, the potential adverse consequences for individuals, however serious or substantial these are and how likely they are to happen. Some data security breaches will not lead to risks beyond inconvenience to those who need the data to carry out their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered. While these types of incidents can still have significant consequences the risks are very different from those posed by the loss or compromise of Category A and B personal data which may be used to commit identity fraud.

d. **Notification (Informing Data Subjects)**. Notification can be an important element of breach management strategy, although it is not always proportionate. Notification must have

[40] Army WARP and Army Data Protection Support Team (DPST) sit side-by-side in Security Branch, D Info, Cyber & Security, Army Headquarters. On receipt of the initial report, Army WARP will inform Army DPST. If necessary, DPST will inform Commercial partners in respect of a breach concerning Army 3rd Party Suppliers.
[41] The permanent record is retained by Army WARP for 75 years (JSP 441 Part 2 Guidance, Records 05, Annex A refers) which includes Annex B and Annex C to this document.
[42] JSP 440 (Defence Manual of Security) Part 2 Section 1 Chapter 4 refers

a clear purpose, for example, to enable affected data subjects to take steps to protect themselves or allow appropriate regulatory bodies to take action and/or provide advice. The decision to notify a data subject of a breach, loss or compromise of his/her personal data will be taken by the ADPST on a case-by-case basis. Units/organisations are not to write to a data subject without seeking specialist advice from ADPST. If it is deemed necessary to write to a data subject, ADPST will provide units/organisations with a template letter for notification. Notification letters are not to be forwarded to data subjects without first being checked by ADPST. In exceptional circumstances, ADPST may be required to seek legal advice from the MOD Central Legal Services.

e. **Lessons and Closure**. It is important to evaluate the effectiveness of the unit/organisations response to a breach and learn/identify lessons. For example, a review of policies, processes and procedures may be necessary to ensure continuous improvement and avoid the situation arising again. The Incident Manager is to consider the following and involve stakeholders who would have an action to improve policy, processes and procedures:

(1) Identify weakness in existing policy, processes and procedures.

(2) Whether the PIAO needs to review the Privacy Impact Assessment Document Set (PrIA DS) to improve processes and procedures in the processing of the personal data. Amendments to PrIA DS must be signed off by the PIRM, and personnel using the personal data are to be informed of the adjustments/improvements.

(3) Establish where the greatest risks lie; for example, how much Category C Sensitive Personal Data is held and is it stored across the business or is it concentrated in one location.

(4) Ensure the method of transmission used when sharing or disclosing personal data to others is secure[43], and only the minimum amount of data necessary to achieve output/service is disclosed. By doing this, in the event of a breach, risk will be reduced.

A detailed Lessons Identified Report (Annex C) is to be finalised by the Incident Manager, endorsed by the PIRM, and submitted to the Commanding Officer and Army WARP no later than 1 month after conclusion of the investigation, along with a completed copy of Annex B. Once Army WARP/DPST are satisfied that actions have been completed and lessons have been documented to inform policy, processes and procedures, the unit/organisation will be informed of case closure by Army WARP. The Lessons Identified Report is an auditable record and is to be retained by the unit/organisation for 2 years.

Contact Details of Army Data Protection Support Team:

SO2 DPA	Mil 94393 6755 Civ 01264 886755
SO3 DPA (Assurance)	Mil 94393 6756 Civ 01264 886756
SO3 DPA (Governance)	Mil 94393 6874 Civ 01264 886874

Email: DII: Army Info-CyberSy-DPA-0Mailbox
External: ArmyInfo-CyberSy-DPA-0Mailbox@mod.uk

Contact Details of Army Warning Advice and Reporting Point Team:

SO2 WARP	Mil 94393 6804 Civ 01264 886804
SO3 WARP 1	Mil 94393 7618 Civ 01264 887618
SO3 WARP 2	Mil 94393 6803 Civ 01264 886803

[43] Registered Mail requires a signature at start/end only (greater risk), than using Special Delivery which requires a signature throughout (low risk).

Email: DII: Army WARP-Mailbox
External: ArmyWARP-Mailbox@mod.uk

Appendices:

1. Personal, Protected and Sensitive Personal Data.
2. Data Protection Breach Management - Summary Action Table.
3. Data Protection Breach Management - Lessons Identified Report,

Appendix 1 to
Annex E to
ACSO 2190
Dated May 17

PERSONAL, PROTECTED AND SENSITIVE PERSONAL DATA

(Note: the below lists are not inclusive)

Cat A – Personal Data. Example:

- Name
- Work/Business Address
- Work/Business Email
- Postcode
- Work Telephone numbers
- Date of birth
- Service/Staff Number
- Identifiable Photograph

Cat B – Protected Personal Data. Example:

- Pay, banking or financial details
- National Insurance Number
- Passport Number
- Driving license number
- Performance Reporting (MS) details (OJAR/SJAR/PADR)
- Next of Kin (NOK)/Family Details (spouse/partner/children)
- Home address
- Home email
- Medical Information (eg blood group)
- Record of Service
- Education/Qualification Details
- Welfare information, such as material relating to social services/ child protection/housing
- Tax, benefit or pension records
- Nationality
- Security Clearance
- CCTV

Cat C - Sensitive Personal Data. Example:

- Sexual/gender matters
- Physical or mental health condition
- Religious beliefs or other beliefs of a similar nature
- Political opinions
- Racial or ethnic origin of the data subject
- The commission or alleged commission of any offence
- Any casework or record relating to any offence committed or alleged to have been committed, AGAI 67 proceedings and the disposal of such proceedings or the sentence of any court
- Membership of a trade union (within the meaning of Trade Union and Labour Relations 1992)
- Free Text Boxes (embedded within applications/forms)
- DNA or fingerprints

Appendix 2 to
Annex E to
ACSO 2190
Dated May 17

DATA PROTECTION BREACH MANAGEMENT

SUMMARY ACTION TABLE

Unit Name	
Incident Manager	
Contact Details	
Incident Name and Number	

Ser	Subject	A brief summary of Comments/Action Taken	Timings
1.	**eMSF Report to Army WARP**	*para 5 (a) refers*	*Date of Incident:* *Date Immediate Report to Army WARP:*
2.	**Containment and Recovery**	*para 5 (b) refers*	*Within 24 hours:*
3.	**Damage Assessment Report**	*para 5 (b) refers*	*As soon as possible after initial Containment & Recovery action:*
4.	**Assess Risk to Data Subjects and MOD Reputation**	*para 5 (c) refers*	
5.	**Notification (Informing Data Subjects)**	*para 5 (d) refers*	*On direction from ADPST.*

ADPST will conduct a remote assurance of the units/organisations EUN page on Army Information Asset Register. The unit/organisation data protection governance structure is to assist with action plans generated through remote assurance.

A copy of this table should be submitted to Army WARP, once complete.

LESSONS IDENTIFIED REPORT

Unit Name	
Incident Manager	
Contact Details	
Incident Name and Number	

Ser	Subject	Detailed Description
1.	**Summary of Incident? (Who, What, Why, Where, When, How)**	
2.	**Identify Threats, Vulnerabilities & Risks to be Treated?**	
3.	**Which policies, processes, procedures need to be improved, how is the improvement implemented and by whom?**	Also explain if improvement has been implemented; if not, when will it be?
4.	**Lessons Learnt?**	
5.	**Is there a requirement for re-training and by whom?**	Explain what specific re-training was necessary and when it was completed; if not yet completed explain why?

A copy of this report should be submitted to Army WARP, once complete.