National Offender Management Service

IT Security Policy

This instruction applies to:-		Reference:-
Prisons NOMS Headquarters Providers of Probation Services		**PSI 25/2014** **AI 19/2014** **PI 19/2014**
Issue Date	**Effective Date**	**Expiry Date**
01 May 2014	01 June 2014	For review by 01 May 2015
Issued on the authority of	NOMS Agency Board	
For action by (Who is this Instruction for)	All staff responsible for the development and publication of policy and instructions) ☒ NOMS HQ ☒ Public Sector Prisons ☒ Contracted Prisons* ☒ National Probation Service (NPS) Directorate ☒ Governors ☒ Heads of Groups ☒ Community Rehabilitation Companies (CRCs) ☒ NOMS Rehabilitation Contract Services Team ☒ Other Providers of Probation Services **** If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***	
Instruction type	**Service specification support/ Service improvement/ HR function**	
For information	All staff	
Provide a summary of the policy aim and the reason for its development / revision	The mandatory actions contained within the policy ensure that NOMS and providers of contracted prison and probation services remain compliant with the HMG Security Policy Framework. This policy replaces PSO 9010 – IT Security and a number of separate probation instructions that relate to the security surrounding probation ICT systems and has been updated to reflect the improvements and updates that have been put in place across the organisation around the security of ICT systems. Since the issue of PSO 9010 NOMS has achieved HMG Information Assurance Maturity Model levels 1 and 2 which reflect improvements in processes and procedures for handling information securely. This policy reflects the changes required by the implementation of the new government security classification scheme and the changes to the organisational structure introduced through the TR Programme. Contract Requirements mean that Community Rehabilitation Companies (CRC) are required to comply with ISO27001 Information management Security System; this policy supports those requirements and the mandatory controls within the ISO.	
Contact	Clare Lewis Head of Information Policy and Assurance Team 0300 047 6258	

.

Associated documents	PSI 24 /2014 - AI 18/2014 - P I 18/2014 - Information Assurance policy PSO 9025 – PI 06/2011 Archiving, deletion and retention PSI 12/2014 – AI 10/2014 – PI 04/2014 - Government security classification policy PSI 16/2012 – AI 04 2012 Information risk management policy AI 2014/05 - PSI 2014/07 - Security Vetting policy AI 20/2014 - PSI 27/2014 - PI 23/2014 - Security Vetting – Additional Risk Criteria For Ex-Offenders Working in Prison and Community Settings
Replaces the following documents which are hereby cancelled : PSO 9010 IT Security	
Audit/monitoring: Compliance with this instruction will be monitored by Internal Audit & Assurance. The Director of NPS in England, Director of NOMS in Wales and NOMS Director of Rehabilitation Services for CRCs will monitor compliance with the mandatory requirements in this instruction. NOMS contract management will hold providers to account for delivery of mandated instructions as required in the contract.	
Introduces amendments to the following documents: None	
Notes: ***All Mandatory Actions throughout this instruction are in italics and must be strictly adhered to.***	

.

CONTENTS

Section	Subject	For reference by:
1	Executive Summary	All staff
2	IT Security	
3	Secure use of the GSI/PSN, internet and email	
4	Working away from the office and removable media	
5	Access Control	Information Asset Owners, Asset custodians
6	Risk assessment, risk management & accreditation	
7	Security Incidents	All staff
8	Asset controls	Information Asset Owners, Asset Custodians
9	Virus Protection	
10	Disaster recovery & contingency planning	
11	Data backups	All staff
12	IT Equipment & removable media disposal	
13	Connection of NOMS systems to other systems	Information Asset Owners, Asset Custodians
14	Installation of non centralised systems	
15	Wireless local area networks, mobile telephone & internet services	
16	Prisoner access to IT equipment and systems	All staff
17	Security Operating Instructions	
Annex A	Guidance on the correct use of the internet	
Annex B	Inappropriate use of the internet and IT systems	

1. Executive Summary

Background

1.1 The aim of the Policy is to ensure adequate protection of all NOMS IT assets, comprising of computer hardware and software, telecommunications and all data retained within NOMS provided IT Systems safeguarding the confidentiality, integrity and availability of official data. The mandatory actions contained within the policy ensure that NOMS and providers of contracted prison and probation services remain compliant with the HMG Security Policy Framework.

1.2 The policy has been updated to include references to the new government security classification scheme throughout as well as references to the National Probation Service and Community Rehabilitation Companies. This policy replaces PSO 9010 and existing Probation IT Security policies.

1.3 The previous IT Security policy was issued in 2009 and is now out date in some areas, in particular the requirements regarding the use of removable media, guidance on remote working and the accreditation of IT systems.

1.4 The policy has been updated to provide clear guidance to all users of NOMS IT, Information Asset Owners and ICT Information Asset Owners as to what they should do in order to meet HMG requirements for managing NOMS IT systems securely as set out in the Security Policy Framework (SPF). These are not new requirements for NOMS as they already form part of the current requirements but the aim of this policy is to enable staff and managers to comply with mandatory requirements. Community Rehabilitation Companies are required to comply with ISO27001: Information Management Security System; this policy supports those requirements and the mandatory controls within the ISO.

Desired outcomes

1.5 To make users of NOMS IT aware of their responsibilities, authority and accountability in respect of the use of NOMS IT systems, IT equipment and the Internet, and what is deemed to be inappropriate use.

Application

1.6 *Users of NOMS supplied computer systems and those IT systems supporting NOMS business processes must comply with regulation, NOMS policies and all relevant HMG and MoJ policies.*

Mandatory actions

All Mandatory actions within this policy are shown in italics.

1.7 Governors, Directors of Contracted Prisons, Deputy Directors of Probation, Heads of Community Rehabilitation Companies, Heads of Groups providers of probation services, contractors, third party suppliers and delivery partners *and Information Asset Owners must ensure that Senior Management Teams and Information Asset Custodians review and are aware of this policy and comply with the mandatory requirements set out in it..*

Resource Impact

1.8 There will be some resource required for the risk management process surrounding the accreditation of IT systems and the renewal of this assurance:

1.9 For national systems the accreditation, patching and upgrades this work will be resourced by the CICT Directorate. ICT IAOs are responsible for ensuring annual reaccreditation takes place.

1.10 *For new ICT systems the accreditation will form part of the implementation of the project and the resources must be included in the project costs.*

1.11 For local systems in prisons and headquarters where an application cannot be moved onto centrally accredited systems such as QUANTUM and where the IT contains sensitive and/or personal information, Athena IT managers will support governors, to complete a Self Accreditation Questionnaire if they have not already done so. There will be a resource requirement to carry out this work which will be dependant on the number of locally purchased IT systems that are in place. The questionnaire will take a maximum of 1 hour to complete.

1.12 It is unlikely that once the questionnaire has been completed the local systems will require full accreditation because all highly sensitive data should currently be held on accredited systems such as QUANTUM or on stand alone IT such as a laptop with the appropriate level of encryption however there may be a requirement to purchase up to date anti virus protection, if the current cover has lapsed, or provide some level of encryption software to provide the correct level of protection to the data held on the IT system.

1.13 For the National Probation Service where local IT systems have transferred ownership to NOMS, the risk management process will be carried out as part of the TR programme of work and will be funded centrally. Where the local IT systems have transferred to the CRCs it will be the responsibility of the CRCs to ensure that they have the appropriate security controls in place.

(Approved for publication)

Ben Booth
Director Change and ICT, NOMS

2. IT Security

2.1 As an executive agency of the Ministry of Justice, the National Offender Management Service (NOMS) has delegated responsibility for its own IT Security Policy.

2.2 NOMS, in line with current legislation and standards, Cabinet Office and Ministry of Justice policy and advice and guidance from other relevant Government Agencies aims to ensure adequate protection of all IT assets. The scope of IT assets comprises of computer hardware and software, removable media, telecommunications and data retained within those systems and the aim of this policy is to safeguard the confidentiality, integrity and availability of official data.

2.3 The result of failure to comply with these mandatory instructions could be unauthorised access or attempts to access a computer system: deliberate unauthorised disclosure; alteration, deletion or use of data which may constitute a criminal offence

2.4 Such failures may lead to protracted disruption and may be followed by disciplinary action, prosecution and or civil restitution.

2.5 For the purposes of the policy, the terms ”IT system”, “computer system”. “systems” and “equipment” mean any computer or microprocessor based system, computer, communications network or other device used for storing, processing or otherwise accessing or disseminating any official information.

2.6 Business Partnerships and Third Party Suppliers

The policy also applies to contracted personnel, business partners and third party suppliers handling and processing NOMS data and maintaining IT systems, including custodial, community and escort service providers.

2.7 *IT service providers and all other IT service providers whose systems are utilised on NOMS sites or to manage NOMS information assets on their own IT systems must comply with this order. This requirement must be reflected in any contractual arrangements with any third parties.*

2.8 The management of the contract with NOMS’ IT service providers and any other contract with a third party supplier, including Community Rehabilitation Companies, may require supplementary procedures to be adopted by NOMS staff.

2.9 All third party suppliers to NOMS such as Library, Educational, Resettlement and Catering Services are required to submit their IT systems in use at NOMS locations, their premises and their suppliers premises where information relevant to the provision of the contracted services is held or processed or where the systems are supported, for risk assessment and subsequent negotiated risk mitigation actions. The demonstration of compliance with ISO 27001 Information Management or alignment and adherence to this policy, the Information Assurance Policy, Data Protection Policy and the Retention, Archiving and Disposal policies will be sought.

2.10 Security Clearance

All staff and contracted personnel, business partners and third party suppliers handling and processing NOMS data and maintaining IT systems must be security cleared to a proportionate level relevant to the security classification of the data being processed or sensitivity of the supported business process or unit.

2.11 *Ex-offenders subject to the limited and time bound Standard Plus vetting level must only have limited and controlled ICT access, dependant on a local assessment of risk.*

Further details and guidance on the levels of clearance required can be found on My Services or in the Security Vetting Policy - AI 2014/05 - PSI 2014/07

2.13 Government Security Classification (GSC) Scheme

All staff need to understand the requirements for the handling of information held in electronic format on IT systems. The marking of the information and the where appropriate the IT hardware is determined by the impact of a potential compromise of the asset as well as any threat to the confidentiality of the information held on the IT. Compromise being the accidental or deliberate violation of asset confidentiality due to, unauthorised disclosure, loss, theft, destruction, tampering, deliberate or accidental modification.

2.14 The new Government Security Classification system has removed the protective markings of UNCLASSIFIED, PROTECT, RESTRICTED and CONFIDENTIAL from new information created after April 2014 and has replaced them with the security classifications OFFICIAL, SECRET and TOP SECRET. Previously marked information and IT assets do not need to be marked retrospectively. It is expected that staff fully understand the impact of compromise of the data and will handle the data accordingly as responsible and professional custodians.

2.15 The new classification scheme covers:

- The markings of data processed on NOMS information systems or those business partners systems that have been certified to hold data on behalf of NOMS and the requirements for the handling of protectively marked information
- Information held and used by NOMS which ranges from highly confidential or sensitive through to public information and have different impacts upon NOMS should the information be compromised.

2.16 It is necessary to decide what sort of information is being processed and to protect each set of information with the level of security appropriate to its sensitivity.

2.17 By following this instruction NOMS will minimise the risk of comprising information held on its IT systems and other IT systems used to support its business processes

2.18 The confidentiality, integrity and availability of all NOMS information must be assured therefore all staff / users must be familiar with the handling requirements of marked information assets stored or processed on IT system or devices including:

- *data stored or processed in information technology systems*
- *data transmitted on networks or telephone lines*
- *data held on removable media e.g. laptops, Blackberry's, smart phones, tablets, hard disks, CDs, DVDs, mass storage devices, memory cards and sticks and other memory storage devices.*

2.19 There is no requirement for an electronic file, within a system accredited to hold information with that marking, for data to be electronically marked. There is no mandatory security requirement for the security classification to be displayed on screen; however, there may be a functional requirement for this to be done in some instances. For other markings seek guidance from the IPA team

Detailed explanation of the new Information Marking and your responsibility to comply with the instructions can be found on the IPA team's intranet pages and in PSI 12/2014 – AI 10/2014 – PI 04/2014 Government Security Classification Policy.

3. Secure Use of the Government Secure Intranet (GSI), Public Services Network, Internet and E-mail

3.1 The purpose of this section is to guide staff and other authorised users of NOMS IT systems on the appropriate use of NOMS e-mail and access to officially supplied Internet accounts for accessing the Internet either directly or through the Government Secure Intranet (GSI) / Public Services Network (PSN). This access includes the use of any NOMS computer and further includes any access to the internet through third party owned computers from NOMS premises or across NOMS networks. Internet access will generally be achieved solely via the GSI/PSN.

3.2 These systems have been supplied for use in relation to your work, but reasonable private use, not involving commercial gain or other inappropriate activities, is permitted, as long as it does not interfere with the performance of your duties and does not take priority over work responsibilities, is in compliance with this policy and NOMS policies generally.

3.3 It is important that all staff using e-mail and the Internet are seen to be using it responsibly at all times. Users should be aware that e-mail usage and access to Internet sites may be monitored.

3.4 Failure to comply with the rules and guidance set out in this Policy may result in legal claims against you and the organisation and lead to disciplinary action being taken against you. Such action might result in your dismissal.

3.5 *Access to the Internet must only be gained on officially supplied hardware via the GSI/PSN, except by specific agreement of the NOMS Director of CICT after submission of a risk assessed business case, such risk assessments are to be managed by the IPA Team*

3.6 *The e-mail system and access to GSI/PSN and the Internet must not be used in ways which could expose the network to hostile attack, cause offence to other users or cause damage to the reputation of NOMS.*

3.7 *Access to social media sites must only be done so within the controls set out in NTS 2013/25 – Using Social Media Responsibly.*

Personal Web mail accounts such as Hotmail or Gmail must not be accessed or used on any NOMS system.

3.8 *Staff using the GSI/PSN, Internet and e-mail must be aware that any inappropriate use of NOMS communications systems whether under this policy or otherwise may lead to disciplinary action being taken against them which may lead to dismissal.*

The GSI/PSN is monitored to notify managers when it is under attack or being maliciously scanned by hackers.

3.9 NOMS will not routinely monitor personal communications. However, NOMS may employ monitoring software to check on the use and content of e-mail to ensure that there are no serious breaches of the policy. NOMS specifically reserves the right to authorise personnel to access, retrieve, read and delete any communication that is created on, received through or sent via the e-mail system.

3.10 Any information stored on a computer, whether on a hard disk or in any other manner may be subject to scrutiny by NOMS. This examination helps ensure compliance with internal policies and regulations. It supports the performance of internal investigations and assists the management of information systems.

Staff must not store personal information, including photographs, on NOMS IT systems.

3.11 Part of a manager's role is to continually assess staff performance and to make themselves aware of any factors that may be affecting it. They will, therefore, as they do for other private activities taking place in the workplace, observe use of IT systems and assess whether excessive use is adversely affecting the performance of their staff.

Further guidance on the appropriate use of email, secure email addresses and managing misuse of the GSI/PSN can be found in the Annexes of this policy.

4. Working away from the office and removable media

Further detailed guidance can be found in the NOMS Remote Working and Mobile Computing Security Guide.

4.1 Working away from the office

You may be working remotely from:

- Another departmental office;
- Home; or
- Any other location, such as while travelling, from a hotel or from other public locations

4.2 Information held and used by NOMS ranges from highly confidential or sensitive through to public information, with varying degrees of sensitivity between the two extremes. *The confidentiality of sensitive information and the integrity and availability of all NOMS information must be ensured.* This section describes how to protect officially supplied portable IT and communications equipment from the principal security threats when away from the office.

4.3 Mobile computing is the use of portable computing equipment. Mobile computing equipment is evolving rapidly. Examples of mobile computing equipment include:

- Laptop computers
- Notebook computers
- BlackBerrys and smartphones
- Tablets
- Audio and visual recording/playback devices
- Removable storage media

4.4 *Under the Prison Act 1952 (as amended by the Offender Management Act) individuals must have the necessary authority to take certain NOMS information outside of NOMS premises. Where SECRET or TOP SECRET information is being transported written authority must be given by the Governor, Deputy Director of Probation, Head of Group, Information Asset Owner before use of any kind of IT equipment for official purposes away from the office. This authority must be carried whenever individuals leave official premises with portable equipment and must be produced on demand.*

4.5 *Unless you are given permission by your line manager you must only use officially provided IT equipment to process data classified as OFFICIAL. If you have been given permission to use non NOMS IT such as a home computer this must not be used to store or process NOMS information containing personal information about either offenders or staff.*

4.6 *You must only use officially provided and configured IT equipment to connect to NOMS Wide Area Network (NOMS WAN) and access the QUANTUM or OMNI systems.*

4.7 *All users of portable IT systems such as laptops, tablets and Blackberry's must have access to Security Operating Procedures (SyOps) setting out secure procedures in the use of the IT and must ensure that they are familiar with the SyOps for the device they are using.*

4.8 *Data must be backed up regularly according to the individual business need and the back-ups stored separately from the IT equipment they relate to. SyOps and operating instructions must detail specific arrangements for each system.*

4.9 *Individuals must take reasonable precautions to keep official IT equipment and the information it contains safe. Laptop users must use the approved laptop security device, such as the Kensington lock, and follow the instructions for its use.*

When using IT equipment in public places (e.g. train, aeroplane) the screen should be directed such that unauthorised people cannot read it

IT equipment processing sensitive data must not be used in public places

4.10 *Effective password procedures must be in place that includes password complexity, change frequencies and handling procedures. Further advice can be given by the NOMS IPA Team. Where any device offers a password facility, the default factory settings must be changed*

4.11 Officially provided devices must not be used by any person not authorised to do so (including family and friends).

4.12 Equipment must be stored and transported separately from remote access security devices such as RSA tokens.

4.13 Any laptop or tablet provided by NOMS must conform to an authorised build. No software should be loaded on to the IT equipment without the approval of a representative of the IT service provider who is authorised to give such permission

4.14 Only officially sanctioned communication devices and services can be used with officially supplied IT equipment on NOMS premises. This may include broadband routers used to access the NOMS laptop secure laptop broadband services.

4.15 *All IT equipment must be marked with an asset number and recorded in a local IT asset register*

4.16 Removable Media

Removable media such as CDs, DVDs, and mass storage USB memory sticks (sometimes called dongles) are a particular risk due to their small size yet ability to carry large (increasingly extremely large) amounts of data. This section outlines arrangements for the secure portable storage of electronic information up to security classification OFFICIAL (including information marked OFFICIAL SENSITIVE)

4.17 The required method of portable data storage is to use specific secure password protected and automatically encrypting memory sticks. Details of the current approved device(s) can be found on the IPA team NOMS intranet page.

4.18 *All storage media (other than integral hard disks and the approved portable storage devices) must be physically marked with the full label of the highest protective marking. If media contains OFFICIAL - SENSITIVE data for instance the media must be marked as OFFICIAL -SENSITIVE. When a hard disk is removed from a computer and is retained on site for repair or destined for disposal, it is to be physically marked with the full label of the protective marking.*

4.19 All data must be encrypted when stored on removable media – further advice can be sought from the NOMS IPA team. Wherever possible removable storage media must be locked away when not in use.

4.20 *Where there is a requirement for data from NOMS systems to be stored on alternative media such as CD/DVD this must be formally agreed by the Information Asset Owner/Custodian and the data encrypted or password protected appropriately.*

4.21 In order to ensure the safe transport of NOMS data the issue and return of each item of removable media i.e. laptop, memory stick must be recorded and accounted for six monthly

and recorded on the IT Manager's asset register. The device must be returned to the governor, deputy director of probation, head of group or information asset owner when no longer required for official purposes or when staff leave the post for which the IT was supplied

4.22 If you need to transport information with a security classification SECRET or TOP SECRET, you must seek the advice of the IPA team or the Department Security Officer.

4.23 Loss or theft of any type of removable media or mobile computing device must be reported immediately to the IT Helpdesk as a security incident and to the IPA Team on incidentreporting@noms.gsi.gov.uk or 0300 047 6590.

4.24 Anti-virus Software on mobile computing devices

A reputable virus checker must be installed and must be regularly updated. Our core Suppliers such as HP/Steria are responsible for providing anti-virus software for all hardware provided under the NOMS contract.

Users must ensure they dock their laptops regularly to update anti virus software.

For non-NOMS hardware, procedures must be in place to ensure virus protection is effective.

4.25 Repairs to mobile computing devices

NOMS IT equipment must only be repaired by an authorised engineer, arranged through an approved service provider.

All repairs for NOMS supplied IT must be via the appropriate HP/Steria Helpdesk

All repairs should be supervised to make sure that the engineer does not read or copy information

If the IT has been used for protectively marked information the Hard Disk Drives must not be taken off-site by the engineer unless specifically authorised by the NOMS IA Team.

4.26 Travelling in the United Kingdom

IT must not be exposed to extremes of temperature (i.e. in the boot of a car in winter).

Portable IT must be transferred into the boot of a car in a public place when the car is about to be left unattended.

4.27 Travelling Abroad

If it is necessary to take NOMS supplied IT equipment whilst travelling abroad the following controls will apply:

- *Permission to take NOMS supplied IT or telecommunication equipment outside of the United Kingdom must be obtained from the Governor, Deputy Director of Probation, Head of Group, Head of CRC from the MOJ Operational Security Team.* Advice can be obtained from the IPA team
- Permission will only be granted after a risk assessment by the MoJ IT Security Team.
- Local electricity power sources should be checked – a power source delivering the wrong voltage or a variable supply causing power surges can result in data corruption.

5. Access Control

5.1 All NOMS computers must have adequate access control. A password is one of the simplest ways of protecting the information on your computer against unauthorised access and can be used at several levels.

5.2 Portable devices must have a password at the boot up stage(when starting the device)

5.3 *Access to networks such as NICTS/OMNI must have a password to support the User Identification*

5.4 Depending on the sensitivity of the data being processed it may also be necessary to protect the data at the application and file levels i.e. access to Offender Management systems or to specific sensitive files such as investigations.

5.5 As a minimum Passwords must contain a mixture of letters and numbers.

5.6 Never disclose passwords to any other person, whatever that person's status. Do not use someone else's password.

5.7 *Users of assisted technology who have a legitimate requirement to share their password must obtain permission from Information Asset Owner of the system.* The IPA Team will be able to provide advice if this permission is required.

5.8 Passwords must be changed regularly in compliance with the relevant SyOps or other operating instructions for the device/application.

5.9 When the password is changed it must be changed totally. It is not satisfactory to change only one or two characters.

5.10 Never use sequential keyboard characters (QWERTY, 123456 etc.), a name, part of an address, vehicle registration mark or other detail that can be associated with you, your office or the system itself.

Do not write passwords in notebooks, desk diaries or leave them in any other easily accessible place.

5.11 If password compromise is known or suspected it must be treated as a security incident and reported to the IPA team at incident reporting@noms.gso,gov,uk or on 0300 047 6590. Every effort must then be made to change the password at the earliest opportunity.

5.12 When not using your desk top device and at the end of a work period, however short that period may be, always log-out to prevent unauthorised access by another person.

5.13 Never allow other users access to the system via your login identity. This is to ensure the integrity of your actions are maintained within any system logs and any security incident can be appropriately attributed to the correct User.

6 Risk Assessment, Risk Management & Accreditation

6.1 All information and information systems are assets which have value and consequently need to be suitably protected to ensure business continuity, minimise business damage and maximise efficiency and effectiveness of its use within NOMS. This protection will preserve the confidentiality, integrity and availability of information as part of the delivery of the business process.

6.2 *All IT systems that process NOMS data must be the subject of a risk assessment and where appropriate accredited. It is the responsibility of the ICT information asset owners of national systems to ensure that a valid risk assessment has taken place and that this is reviewed on a regular basis.*

6.3 *It is the responsibility of the governor, head of group, deputy director of probation to ensure the appropriate levels of risk assessment have been carried out for local IT systems, this may include full accreditation or the completion of a self assessment questionnaire. Further advice can be obtained from the IPA team.*

6.4 *Further risk assessments must be carried out when there are significant changes made to the system. This includes upgrading, re-location, re-allocation or disposal of the systems software or hardware.*

NOMS requires effective protective security through the application of risk management.

6.5 Risk Management

Risk management is a structured, common sense approach to providing cost effective and relevant protective security for all protectively marked assets. It involves the identification, selection and adoption of protective controls based on the risk assessment and the sensitivity of information or other valuable assets.

6.6 These controls may be achieved through a combination of technical and non-technical measures. Technical measures are those such as identification and authentication controls, non-technical measures include personnel, physical and environmental controls.

6.7 Risk management is a continual process as asset values, threats, vulnerabilities, protective controls and the degree of acceptable risk do not remain static.

6.8 Risk assessments may be carried out by named individuals locally after instruction from a member of the MOJ Technology IA Team. Assessments will be limited to those areas and systems specified by MoJ IT Security. This may include a part of the overall assessment such as the local controlled risks of a nationally assessed system or application.

6.9 Accreditation

Accreditation is part of the risk management process and provides assurances to the NOMS Senior Information Risk Owner (SIRO) that any risks associated with an information system can be effectively managed. The MoJ Accreditation Framework will be followed in all instances of Accreditation.

6.10 'Accredited' indicates that the MoJ Accreditor has been satisfied that appropriate security measures are in place and has given approval for the system to be operated from the point of view of security.

6.11 *All NOMS and its business partners Information systems processing and storing official information must undergo Security Accreditation.*

Guidance on non centrally supplied IT can be found in Chapter 14 and should be followed in all cases.

7 Security Incidents

7.1 To ensure that an appropriate and ongoing risk assessment process is maintained thereby assuring that NOMS data and systems are protected properly. Effective management of security incidents are important to ensure that the incident is contained, appropriate actions can be taken and lessons learnt can be taken forward including maintaining any forensic evidence that may be necessary if criminal activity has taken place.

7.2 Any suspected security incident must be reported to the IPA team at incidentreporting@noms.gsi.gov.uk or on 0300 047 6590.

7.3 NOMS IPA Team will inform GovCertUK, for further investigation, of any significant security incidents impacting upon the confidentiality, integrity and availability of NOMS Information Systems

8 Asset Controls

8.1 *To maintain the appropriate level of protection, IT assets hardware and software must be accounted for.*

8.2 IT assets fall into 3 categories:

- Information assets (databases and data files, system documentation, user manuals, training manuals etc)
- Software assets (application software, system software, development tools etc)
- Physical assets (computer equipment, communications equipment, magnetic media etc)

8.3 *Only officially purchased and properly licensed software can be used on NOMS IT Systems and those in use on NOMS premises. The terms and conditions of the license must be adhered to.*

8.4 *No member of staff, prisoner or anyone else can copy software unless appropriate licenses are in existence.*

8.5 An asset register of all NOMS held IT assets supplied by the relevant authorised suppliers such as HP must be maintained by the supplier

8.6 An asset register of all IT assets must be maintained locally in compliance with the current Finance Policy in regard to NOMS assets and to the same standard for all other systems in use on NOMS premises.

8.7 The asset register must include the following information:

- *Asset number & serial number*
- *Location*
- *Installed software*
- *Licence registration number of installed software*
- *Copy of Invoice and its number and date relating to locally purchased non-core supplier such as HP supplied software*
- *Expiry dates*

8.8 Software Assets

A software licence is required for every copy of any software product operating at any NOMS premises whether a permanent or temporary site. Failure to do so may breach compliance with the Copyright Designs and Patents Act 1988 and may result in heavy financial penalties.

8.9 For locally purchased software licences the governor, deputy director of probation, or head of group, is legally responsible for ensuring that all software in use on all locally purchased IT assets in permanent use on the premises is properly licensed for use. Proof of purchase must be retained in order to meet industry standard requirements for title ownership.

8.10 Local Management must satisfy themselves that software not purchased by NOMS but in use by offenders, contractors and suppliers including CRCs, Education, Health and Library Service providers is properly licensed for use on NOMS premises.

8.11 Particular attention must be applied to Shareware and Freeware utilised for Education and Accessibility needs. These types of software do have license requirements when used by organisations rather than the individual.

8.12 Licences for centrally provided software, such as Microsoft Office on the QUANTUM/OMNI systems will be the responsibility of MOJ Technology.

9 Virus Protection

9.1 Effective precautions must be taken to prevent computer equipment from being affected by computer viruses, as the cost of restoring an infected system can be very high.

9.2 All IT systems must have up to date anti-virus software installed.

9.3 Locally provided IT hardware must have local procedures in place to ensure anti-virus software is installed, maintained and updated in all equipment. Additionally they are responsible for adequate firewalls and malware protection of any standalone IT

9.4 Virus protection for centrally provided systems such as the QUANTUM/OMNI systems will be the responsibility of MOJ Technology.

Roaming users must ensure they dock their laptops regularly to update anti-virus software.

All removable storage media must be virus checked before use. Contact the IPA team or your IT Manager for advice on how to do this

9.5 If virus infection is suspected the following actions must be taken:

- *Stop work, do not attempt to use the suspected workstation*
- *Do not attempt to take any action against the virus*
- *Do not switch off the workstation*
- *Remove any removable media from the workstation (be aware that the media itself may be infected)*
- *Immediately inform the relevant IT HP or Steria helpdesk or the appropriate service provider for advice*
- *Report the occurrence as an IT Security Incident to the IPA team at incidentreporting@noms.gsi.gov.uk or on 0300 047 6590.*

10 Disaster Recovery and Contingency Planning (DRCP)

10.1 *All NOMS computer systems must have a plan in place to ensure that acceptable levels of service, control and security across the organisation can be maintained in the event of a disruption to computing services*. Disaster Recovery and Contingency Planning (DRCP) is the process to manage and recover from a major incident. An IT Business Continuity Plan is the alternative or manual process applied in the event of an IT failure. Our relevant main suppliers such as HP and Steria supply a local Business Continuity Plan for all strategic systems and are responsible for the disaster recovery capability for all equipment supplied under NOMS contract.

10.2 *Business Continuity Plans (BCP) must exist for all IT systems and be tested on a regular basis. Information Asset Owners for central IT systems are responsible for ensuring appropriate business continuity plans are in place for their IT system and plans are reviewed on an annual basis.*

10.3 BCP, DRCP, and IT Contingency Plans must be integrated into site contingency plans and must be held in a secure location remote from the equipment to which it relates.

11 Data Backups

11.1 Data backups are taken to ensure business continuity in the event of an IT failure, including all networked and standalone computer systems. Care should be taken to include all business critical systems in the backup routine, including those services provided on site by business partners such as Healthcare.

11.2 *Backups of all official data must be taken at regular intervals according to the business need and indicated by the SyOps*

11.3 If the system that is being backed up contains any sort of personal information the backup devise used must have the appropriate level of encryption / password protection.

11.4 Backups of local systems must be stored in a fireproof container, remote from the computer system to which they relate. Backup storage areas should be accessible in the event of a serious incident on site such as fire or flood. Local Contingency plans should include instructions for the safe retrieval of backups to the business continuity facility.

11.5 *A back up log recording details of who made the backup, what was backed up and the date the backup was taken must be maintained and stored securely.*

11.6 National systems such as QUANTUM/OMNI will have their own backup process in place which must be adhered to

12 IT Equipment and Removable Media Disposal

12.1 *During all stages of data handling, protection against loss, disclosure or corruption must be ensured.*

12.2 All stages of the media disposal process must have an auditable management trail, which documents details of the disposal and must comply with the mandatory requirements in the Retention, Archiving and Disposal policy .

All media prior to disposal must be held in auditable secure storage.

12.3 All IT media, including disks, tapes, hard disks, CD-ROMs, memory stick etc., must be disposed through a NOMS recognised disposal organisation. The current contractors are listed in the IPA team pages of the NOMS Intranet.

Centrally provided IT will be disposed of by the relevant supplier (HP/Steria)

12.4 All items for disposal must be collected from site by the contractors unless alternative arrangements are approved by the NOMS SIRO. It is not permitted to send any item for disposal via any mail or courier service without the approval of the NOMS SIRO.

12.5 Request for the removal or disposal of core contract NOMS equipment should be dealt with under the IMAC procedures. These can be found on the Intranet under NOMS and in PSO 9030 'Handling and Approval of Requests for IT/Telephony Business Requirements'.

13 Connection of NOMS systems to other systems

13.1 The security of NOMS IT systems must be maintained against unauthorised access that compromises the confidentiality, integrity or availability of such systems.

13.2 Connection of any network to another presents risks that must be minimised or eradicated.

All requests for dial up or broadband access that will be connected through any NOMS telephony system or telephone/broadband line must be agreed formally by local management who must seek the advice of the IPA team.

13.3 No NOMS computer system or network may be connected to another without the appropriate risk assessment having been performed by the MOJ Technology IA team and countermeasures implemented to minimise the identified risks and vulnerabilities.

13.4 Separation must be maintained between NOMS systems and all others. It is not permissible to share network infrastructure installations such as cabinets etc without the approval of MOJ Technology IA.

14 Installation and use of non centralised systems

14.1 *The security of permanent non-centralised systems in use at NOMS premises must be maintained against unauthorised access that compromises the confidentiality, integrity or availability of such systems, and that their use complies both with the owners and NOMS policies for use i.e. the use of computing facilities by contractors, agency staff and engineers etc*

14.2 In order for NOMS business partners and service providers to meet their contractual obligations and for NOMS to ensure best value from contracts and other working agreements and where it has not been possible to offer access through NOMS infrastructure due to technical, security or volume concerns, or where access to IT systems is required by prisoners, there will be requirements that must be met for the installation and use of non NOMS systems on NOMS premises. An example of this could be IT systems used by healthcare providers or education

14.3 All such systems will carry their own risks and each site will have its own requirements due to its nature and role. *It must not be assumed that because a system is installed and in use at one site that the same system or one similar to it will be acceptable at any or all others.*

14.4 All non-NOMS systems and installations must be subject to a Risk Management Assessment by MOJ Technology IA and must be accredited in accordance with the MoJ Accreditation Framework

14.5 All non NOMS systems major components must be physically separated from NOMS systems and shared cabling arrangements must be formally agreed to by the IPA team or MOJ Technology IA.

14.6 IT Systems that are not officially supplied and/or managed by core NOMS suppliers such as HP/Steria but that are locally procured by NOMS staff for the purposes of their business must have a System Owner identified in order for them to ensure compliance with this policy as well as the legislation and regulations surrounding the management and processing of personal data and system management.

14.7 System Owners of IT systems that are independently procured will be responsible for ensuring that the system fully complies with this policy and be held accountable for any security incidents relating to data or system breaches. System breaches will include but are not exhaustively defined as:

- *Password breaches*
- *Account breaches such as sharing or unauthorised access*
- *Integrity breaches – system access by an unauthorised person*
- *System breaches – unauthorised changes in configuration settings i.e. configuring internet access*
- *Data breaches – where the 'need to know' principle is breached and people who have no 'need to know' have access to data.*
- *Connectivity of non core supplier (such as HP) supplied/managed systems to official systems*
- *Storage of data overseas*
- *Malware intrusion – virus/spam etc…*

14.8 All breaches must be reported to the NOMS IA team at incidentreporting@noms.gsi.gov.uk or on 0300 047 6590 as soon as possible.

14.9 System Owners must ensure that an appropriate risk assessment is carried out before authority is given by the System Owner to operate. Failure to do so will put any data that is

stored at risk as well as potentially compromising the systems functionalities and services. An independent assessment called the Short Assessment Questionnaire (SAQ) must be conducted by the System Owner to assure the system does not require a more comprehensive assessment and that security controls are in place and are appropriate. The SAQ is available from the IPA Team.

14.10 It is important to ensure the scope of the SAQ or approved risk assessment takes into consideration the whole scope of the service provision which is being offered including support and storage arrangements, licence management

14.11 Once completed, the SAQ or the other approved risk assessment process should identify risks that the System Owner should document and record on an appropriate risk register and manage in accordance with corporate risk management processes and procedures. Any major changes to the system will inevitably produce potential risks and a review of the SAQ or approved risk assessment process must be carried out. This should then be recorded and managed appropriately. Failure to comply with this may lead to breaches in security and improper usage of the system.

14.12 A record of the risk assessment(s) must be made available during the lifetime of the system for audit and evidential purposes. This must be accompanied by the relevant documentation required by this policy such as the SyOps.

14.13 Other considerations that must be assessed by the System Owner will be but not limited to include:

- *Privacy Impact Assessment*
- *Information Sharing Agreements that need to be in pace before a third party can have access to NOMS data.*
- *Security clearances for third party staff*
- *Information Asset Register update and accurate recording.*
- *Internal Audit considerations for Information Assurance.*
- *Decommissioning the system securely once end of life*

15 Wireless local area networks (LAN), mobile telephone and internet services

15.1 Due to the increasing availability of equipment and technical information to enable interception activities, all data carried on wireless LANs should be considered vulnerable to interception. As well as interception, wireless communications are susceptible to jamming. Mobile telephones are often the target of opportunist theft. The following matrix details the standard for the digital communication of marked information.

	Business Impact Level			
Method of Communication	IL0	IL1, IL2	IL3	IL4
NOMS Internal Phone Service - Internal Calls	Y	Y	Y	N
NOMS Internal Phone Service - External Calls	Y	Y	Y1*	N
External Phone Line (PSTN)	Y	Y	Y1*	N
Mobile Phone (GSM)	Y	Y	N	N
Bluetooth	Y	Y	N	N
Pager	Y	Y	N	N
Fax Machine	Y	Y	Y2*	N
NOMS Email Service	Y	Y	Y	N
Internet Email Service	Y	Y	N	N
Blackberry	Y	Y	Y	N
Brent Secure Fax/Telephone	N	N	N	Y

Notes
1* Use guarded language
2* Ensure recipient fax no is bona fide

15.2 Wireless LANs (WiFi) must be considered to be highly vulnerable to interception and jamming and the advice of the MOJ Technology must be sought before a wireless LAN solution is considered.

15.3 Mobile telephones must be considered highly vulnerable to interception and jamming and must not be used where communications contain very sensitive information. Guarded language should be used at all times as communications may be vulnerable to interception.

15.4 All instances of wireless communication including' line of sight' and satellite must be subject to risk assessment by MOJ Technology IA.

15.5 Bluetooth can not be used except under formal assessment and agreement of Security Group and MOJ Technology IA.

15.6 The address book and message facilities in mobile phones and messages on pagers should be protected from unauthorised access at all times

15.7 All mobile communication devices must be protected by utilising the PIN lock number must be changed from the factory preset.

16 Prisoner access to IT equipment and systems

16.1 NOMS has a responsibility to regulate prisoner and offender's in the community access to IT, IT services and information and communication facilities and access to digital information and assets whilst maintaining NOMS policies in respect of security, harassment, detection and prevention of crime.

16.2 This will include providing standards for the introduction of NOMS authorised IT systems for prisoner and offenders in the community use. Including but not limited to games consoles, digital TV equipment, video conferencing, audio visual players, IPTV systems and systems delivering education, learning and skills and resettlement services. Specific requirements in respect of these systems and their use including in possession and in-cell can be obtained from Security Group.

16.3 Prisoners and offenders in the community must not be allowed access to any IT or IT system not specifically provided or authorised for their use.

16.4 Prisoners and offenders in the community will be provided with IT in accordance with the current access to justice policy.

16.5 Prisoners must be assessed per current National Security Framework instructions before being granted access to IT equipment or systems whilst in custody.

16.6 Access to the Internet by Prisoners

The basic principle that applies to all forms of communication – preventing the transfer of information that might aid crime, threaten prison security or aid escape from custody and the protection of victims must be applied with regards to Internet access for prisoners and offenders in the community.

16.7 Access to Internet facilities may allow prisoners or offenders in the community to abuse [or harass] victims either through direct, electronic communication or by indirect proxy contact outside the prison and these considerations must be weighed against any perceived advantages.

16.8 The risk exists that prisoners could use the Internet to commit, prepare for or encourage crime whilst in custody. Additionally they could access material that might endanger the security of the prison e.g. access to bomb-making techniques.

16.9 The accessibility of learning materials by prisoners in custody must be balanced against security considerations. Access to the Internet will only be granted following a thorough risk assessment on a case-by-case basis of the system, hardware, software and connectivity. Prisoners access to IT whilst in custody is subject to individual assessment as per the National Security Framework and advice on appropriate access controls can be obtained from security group, the IPA team..

16.10 Prisoners must not be allowed uncontrolled access to the Internet and/or to a computer or IT system whilst in custody that has software installed enabling Internet connectivity without seeking approval from security group, the IPA team and the completion of a thorough risk assessment.

16.11 All IT systems providing internet access for prisoners must be risk assessed by the MOJ Technology IA prior to prisoner access being granted.

16.12 All prisoners must be subject to an individual risk assessment before having access to IT and or electronic storage devices of any kind.

16.13 All IT and electronic storages devices for prisoners use whilst in custody must be subject to an MOJ Technology IA assessment.

16.14 All prisoners must sign a compact whilst in custody detailing the acceptable use requirements of the device and or service.

Further advice can be found in the Prisoner Access to Information Communication Technology (ICT) policy which is owned by Security Policy Unit or contact the Information Policy and Assurance team on informationassurance@noms.gsi.gov.uk

17 Security Operating Procedures (SyOps).

17.1 SyOps are required for all computer systems operating within NOMS and apply to all IT assets owned or operated by NOMS or any other third party supplier to NOMS.

Annex A

1 Guidance on the correct use of E-mail

1.1 E-mail allows us to send messages and attachments to any other e-mail account. It is quick, easy and efficient but should be treated with the same care as any written communication.

1.2 Not only can e-mail messages be read en route but also they can be easily modified or deleted, particularly when transmitted across the internet to third parties. Users cannot be sure that the messages or data originated from the apparent sender or contained the data that the sender intended.

1.3 E-mail messages that have been deleted from the system can be traced and retrieved and so, all persons having a part in creating or forwarding any offending e-mail can be identified. E-mails, both in hard copy and electronic form, are admissible in a court of law.

1.4 Personal use is permitted but users must ensure that use of NOMS e-mail:

- *does not contain or have attachments which contain NOMS information in any format*
- *does not interfere with the performance of their duties*
- *does not take priority over work responsibilities*
- *does not incur unwarranted expense on NOMS*
- *does not have a negative impact on NOMS reputation in any way*
- *is lawful and complies with this policy and HMP policies generally.*

Use of your official work email address is NOT permitted for

- *Purchasing personal items such as from Amazon or Ebay.*
- *Subscribing to social media sites or other services not attributable to NOMS business*

1.5 Personal external e-mails should clearly identify to the recipient that the message is personal and does not express an official view or opinion of NOMS. The following disclaimer must be used :

'This e-mail is confidential and intended solely for the use of the individual to whom it is addressed. If you are not the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this e-mail in error please contact the sender. Any views or opinions presented are solely those of the author and do not necessarily represent those of NOMS. Although this e-mail and any attachments are believed to be free of any virus or other defects which might affect any computer or IT system into which they are received, no responsibility is accepted by NOMS or their service providers, for any loss or damage arising in any way from the receipt or use thereof'

1.6 The disclaimer can be added to e-mail using the signature facility within Microsoft Outlook. If you are unsure how to set up a signature template you should contact the IPA team.

1.7 <u>Sending External E-mails</u>

When sending information by e-mail to persons or organisations outside of NOMS users must ensure the recipient is authorised to receive it and has a legitimate requirement for the information contained within the email. Some intended recipients might have rigorous e-mail gateway protocols (or firewalls), which can automatically screen all incoming e-mail

for content and source or redirect. If this is the case, consider whether this means of communication is appropriate.

1.8 Marking and Sending E-mails containing Marked Information

OFFICIAL (including OFFICIAL SENSITIVE) information must only be sent to addresses with a secure departmental email system. The list below shows examples of secure email addresses but the list is not exhaustive. If you require further information or need to send a sensitive email outside of the NOMS secure email system you should contact the NOMS Information Assurance Team.

The following are examples of addresses for secure systems but this list is not exhaustive:

- a.n.other@justice.gsi.gov.uk
- Division.CJU@dyfedpolice.pnn.police.uk
- another@yjb.gov.cjsm.net
- lawyer01@solicitors.cjsm.net
- A.n.other@nhs.net
- a.n.other@gsx.gov.uk

Sensitive and bulky transmission of personal information will always warrant encryption.

1.9 If the Information Asset Owner is satisfied that the impact of any data compromise would be low enough to warrant a reduction in the controls, information may be sent over the internet to a non secure email address. For the least sensitive material this can be done without encryption or password control, with caution and the appropriate measures to guard against accidental compromise, opportunistic or deliberate attack.

1.10 Applying the Government Security Classification Scheme to emails

Emails that contain OFFICIAL information do not require a security classification to be added to the email

1.11 Emails that contain OFFICIAL - SENSITIVE information must have the word OFFICIAL – Sensitive boldly marked at the top and bottom of the message

1.12 Information marked as SECRET or TOP SECRET ***must not*** *be transmitted over the internet.*

1.13 The automatic forwarding of e-mail to a non-departmental destination is not allowed. Such a mechanism can lead to the accidental transmission of sensitive information.

1.14 Further guidance on transmitting applying the classification scheme can be found in the Government Security Classification Policy

1.14 Functional Mailboxes

Policy relating to Functional mailboxes is contained in PSO 9050 Information on the operation of Functional mailboxes

1.15 All access to the Internet is recorded and saved. Internet usage is regularly monitored by NOMS to ensure that it is not being misused.

1.16 Internet access is for use in relation to your work, but reasonable private use, not involving commercial gain or other inappropriate activities, is permitted, as long as it does not interfere with the performance of your duties and does not take priority over work responsibilities.

1.17 Sites that must explicitly not be accessed include, but are not limited to:

- *personal web-sites i.e. those created and managed by individuals for their own purposes,*
- *sites that feature games or gambling,*
- *sites which contain sexually inappropriate, racist, homophobic or extremist material,*
- *music sites and*
- *pirated software.*

1.18 Prohibited use of the Internet

NOMS systems must not be used to carry out any of the following actions:

- *purchase goods or services on line, unless for official purposes and only when using the Government Procurement Card or when utilising the approved accommodation and travel services.*
- *advertise goods or services of any nature unless this is for official purposes (e.g. information about courses being run by NOMS),*
- *pursue any personal business interest on the Internet,*
- *take part in any mailing lists,*
- *commit any crime, whether or not explicitly mentioned in this guidance, such as hacking (attempted or actual illegal entry to another computer or computer network), forgery or misrepresentation,*

1.19 Only web sites owned by reputable companies or organisations can be accessed by a NOMS user. A reputable company or organisation is defined as one that would suffer loss of face, or a damaged reputation if its site was the source of an attack on a visitor or a visitor's organisation.

1.20 Registering details on remote sites

Many useful sites require you to register to use them. This can result in the site managers using the information to send you advertisements by e-mail. Be careful when providing any details to external sources and supply the minimum detail required to register successfully.

1.21 As a general rule, do not register with mailing lists or for newsletters that are delivered by e-mail. The network may not cope with large numbers of copies of the same file arriving at the same time. You can read copies of the messages in many of these lists on the websites of their hosts.

Inappropriate use of the internet and IT systems

1.1 Potential misuse of the internet identified through automated monitoring

In the case of visits to inappropriate web sites, or other potentially inappropriate use of NOMS system, Governors and Heads of Group and Deputy Directors of Probation will be informed. It is also best practice if a User identifies that they have inadvertently accessed an inappropriate site for them to inform their line manager in the first instance.

1.2 Consideration will first be given to whether circumstances are such as to warrant the individual's access to the Internet and/or NOMS being immediately suspended (eg the circulation of pornographic, sexually explicit, extremist or racist material), pending an investigation. The views of IT Security will be sought to establish whether the activities have involved, or are likely to involve, a breach of security procedures. If immediate suspension of the facility is deemed necessary, the Governor or Head of Group will request IT Security to initiate this.

1.3 The governor, deputy director of probation or head of unit will be asked to ascertain whether there was a need for the site(s) to be visited for official purposes. If this was the case then no further investigation will be required.

1.4 If the visits were not officially authorised, an investigation will be initiated in line with PSO 1300. If further, individual, monitoring is required as part of the investigation, this will be authorised and funded by the governor, deputy director of probation or head of group. In cases involving potential breaches of security, this authority will be given by the IPA team or the Corruption Prevention Unit (CPU).

1.4 Results of the investigation will be forwarded to the investigating officer who will consider further action in accordance with current disciplinary procedures. If a disciplinary offence is proved, the normal penalties will apply. These range from a warning about future conduct to dismissal.

1.5 If it appears that the activities may have constituted a criminal offence, legal advice may need to be obtained before any internal investigation under the disciplinary procedures takes place.

1.6 Potential misuse identified by line management

If a line manager identifies a decline in an individual's level of performance, normal procedures will be followed to identify the reasons and to raise performance to an acceptable level. If excessive personal use of the Internet is a contributing factor, this should be drawn to the individual's attention and normal warnings should be given.

1.7 If a manager observes that an individual's private use of these facilities is excessive or if they observe offensive or other inappropriate material on that individual's screen, normal managerial action should be taken to address these issues. In serious cases, this may mean proceeding immediately with disciplinary investigations.

1.8 If, after the above actions have been taken, the private use of the Internet ceases to be a performance issue and becomes a disciplinary matter, an investigation should be initiated. Where appropriate, as part of such an investigation, further monitoring should take place. Any requests for additional monitoring require authority to be be given by IPA team.

1.9 Results of any investigation will be forwarded the investigating officer who will consider further action in accordance with normal disciplinary procedures.

1.10 The procedures for identifying misuse will be kept under review.

1.11 Sexually Inappropriate & Offensive material

The general principles relating to sexually inappropriate and other offensive material are set out in the sections on harassment, if inappropriate web sites are entered inadvertently use the "Back" button to leave as quickly as possible.

Sexually inappropriate material, gambling sites or other offensive material must not be accessed

1.12 Users of NOMS systems who have a business requirement to access this type of material in the course of their work must obtain permission in writing from their line manage or higher, and all access must be via a standalone computer, provided in accordance with 3.8 above under the authority of ICT and subject to a risk assessment by IT Security.

- *Any separate locally procured and managed Internet access account should not identify the user as a government employee. In particular accounts of the type ".gov.uk" or "gsi.gov.uk" must not be used.*
- *A log or other audit trail must be kept and maintained of any such access.*
- *The impact of inadvertent access upon colleagues not directly involved with this work will also need to be considered - take care when positioning standalone machines to minimise overlooking.*
- *The browser cache should be cleared at the end of each session.*

1.13 Harassment carried out over IT systems

Harassment can broadly be said to include a range of unwelcome behaviour which, whether intentionally or not, creates feelings of embarrassment, humiliation, intimidation or discomfort or causes offence, and/or appears to threaten job security or prospects.

1.14 It is difficult to give an exhaustive list of behaviour which constitutes harassment and the particular context will often be important. The perception of the behaviour by the recipient is often crucial, as is the impact of the behaviour on the recipient. In the context of electronic communication, harassment might include any offensive or intrusive manner of communication, which includes sexually or racially derogatory remarks, innuendo, mockery (e.g. of a disability), lewd or racist jokes, sexually explicit or suggestive material, or intimidating or bullying behaviour towards colleagues. Activities such as the frequent sending of irrelevant messages or sending abusive messages to a person or group of persons (the practices described as spamming and flaming in Internet literature) may also constitute harassment.

1.15 As an equal opportunities employer, NOMS believes that all staff have the right to be treated with dignity and respect. Harassment or discrimination of any kind are unacceptable and can be unlawful. However, the policy extends beyond the purely legal requirements and the Service will view any form of harassment or discrimination very seriously.

Disciplinary measures, including dismissal in serious cases, may be taken against the perpetrator, in accordance with NOMS Policy and Disciplinary procedures.

1.16 Defamation occurring over IT systems

Defamatory comments are ones that cause or are likely to cause serious harm to a person’s reputation, and are sent or shown to somebody other than the sender and the person(s) or company commented about.

1.17 Users may be liable in law for any comments they make regardless of whether NOMS is also liable. Users must ensure that any "facts" quoted are true, and make it clear whenever they are stating a personal opinion. Users should be aware that they might have damages awarded against them if they are held to have defamed someone rather than expressing an opinion about them or to them.

1.18 *The sending of any message that could be taken as defamatory must be avoided*. Placing the message on the e-mail system may be enough for defamation to have taken place.

1.19 Copyright

Copyright is a right of ownership that recognises the intellectual effort that goes into creating a written document, illustration, performance, object, piece of software, music or video etc and protects the copyright owner's rights to benefit from the work. *When viewing pages on the Internet users must assume that they have no rights other than to look at a document displayed on their screen and to print one copy for personal use.*

1.20 Users should be aware that they can send the web address (Universal Resource Locator or URL) of many pages via e-mail to other people who may be interested. In that way users may avoid potential copyright problems, and also avoid storing complex files or sending large files across the network.

1.21 Users and NOMS could be held responsible for a breach of copyright. Damages could be awarded against individuals as a result of any financial losses incurred by the copyright owner because of their actions. In some serious cases breach of copyright is a criminal offence for which individuals can be convicted as well as giving rise to civil liability for which individuals (and organisations) can be sued.

1.22 Entering into contracts via IT systems

A contract exists when a purchaser offers to buy goods or services and the seller agrees to accept the offer. There are strict rules in government about who has authority to enter into contractual relationships and to make purchases generally. This is known as procurement authority and it is different from financial authority. You can easily and sometimes unwittingly enter into a contract by e-mail or through a web site.

1.23 *The rules about purchasing and contracting by e-mail are exactly the same as they are for purchasing by any other means of communication. If individuals do not have authority to purchase or enter into contracts they must not do so.* If individuals do have purchasing authority, then a contract entered into by e-mail or through a web site is equally as binding as one on paper. The only permitted direct internet purchases are those made using the Government Procurement Card.

1.24 Users must not express enquiries in a way that can be interpreted as a contractual acceptance or obligation.

1.25 In particular, neither NOMS nor our main suppliers such as HP/Steria can accept responsibility for financial loss or damage suffered by anyone using NOMS equipment for unauthorised or private transactions over the Internet.

Annex B continued

Contact details and Further Information

- Internal Audit and Assurance and the NOMS information Policy & Assurance (IPA) Team will monitor policy implementation.

- The initial point of contact for additional advice on IT Security is the IPA team at informationassurance@noms.gsi.gov.uk or on 0300 047 6590.\

- The initial point of contact with MOJ Technology IA is ICTIAService@justice.gsi.gov.uk

- Policy advice on Freedom of information and the Data Protection Act is published in PSO 9020

- Policy in respect of Information Assurance and incident reporting is contained within the Information Assurance Policy

- Policy advice on prisoner IT in possession, Access to Justice and prisoner assessment for access to IT is published in The National Security Framework

- The initial contact for policy on prisoner access to PRIS-M, e-mail and other electronic mail systems is the Offender Safety, Rights and Responsibilities unit

- Policy advice on prisoner access to education and resettlement systems and information is available from the Directorate of Commissioning & Commercial