NI Assembly Secretariat Information Assurance - Protective Marking Policy and Procedures

Contents

1. Introduction

1.1 The aim of this policy is to set out the procedures in respect of all matters concerning the use, storage and transfer of information. It establishes a protective marking system to ensure the appropriate application of protective measures is applied to information requiring safeguard.

1.2 The policy relates to information in whatever form it is communicated or stored. This may be in a paper document; however the markings apply equally to electronic media such as word files, e-mails, jpeg images etc. stored on a computer system or information stored on detachable media such as, video tapes, CDs, DVDs or memory sticks. This policy is vital to ensure that information is handled and stored appropriately.

1.3 The Assembly Secretariat seeks to conduct all its business in an open and transparent manner. Most information created will not require a protective marking and therefore will be treated as 'Unrestricted' and will not carry a protective marking to reflect this.

1.4 However, some documents may require a protective marking such as 'Assembly Restricted' or 'Assembly Confidential' to ensure the information is handled in an appropriate manner.

1.5 The objective of protective marking is to manage the preservation of confidentiality, integrity and availability of information.

1.6 It is anticipated that protective markings such as 'Assembly Secret' and 'Assembly Top Secret' will rarely be used. Details of protective markings are provided on pages 6-8.

1.7 A breach of this policy will be considered under disciplinary procedures.

1.8 This policy should be read in conjunction with the Northern Ireland Assembly. **Data Protection Policy**

2. Role of the Senior Information Risk Owner (SIRO) and Information Asset Owner (IAO)

2.1 One person is appointed as the Senior Information Risk Owner (SIRO) for the Northern Ireland Assembly Secretariat.

2.2 Each Directorate will have an Information Asset Owner (IAO). On the Committee side, each Committee Clerk will act as the Information Asset Owner (IAO) for their individual Committee.

2.3 The SIRO will have overall authority in relation to decisions about protective marking and ensuring information risks are assessed and mitigated to an acceptable level. The day-to-day duties may be delegated to the Information Asset Owner (IAO).

2.4 The role of the SIRO and Information Asset Owner (IAO) will include such things as dissemination and monitoring of the policy, type and use of information held in each directorate and responsibility for monitoring use of assets including hardware and software.

2.5 The Information Asset Owner (IAO) should ensure that access to information is managed and up to date records are maintained of staff and privileges as instructed by HR. IAO should ensure HR are informed of any further changes within business areas that may affect access management. Staff movement and access system privileges should be managed in a timely manner and IS Office kept informed of changes to ensure file share permissions are reviewed and, where necessary, revised.

2.6 Security Office should also be informed of any staff changes (staff recruited, staff leaving and staff change of location) to ensure personal details held are reviewed and disposed in accordance with retention and disposal policy.

2.7 The Information Asset Owner (IAO) should pay particular attention to staff leaving the organisation. On receipt of resignation, access to classified information (ASSEMBLY RESTRICTED and above) should be removed and records updated accordingly.

3. NI ASSEMBLY SECRETARIAT PROTECTIVE MARKINGS

UNRESTRICTED
No Protective Marking applied. If a marking is not applied the material will be considered 'Unrestricted'.

ADDRESSEE ONLY
Material only to be seen by the individual to whom it is addressed

EMBARGO
Restriction imposed on the release of information until a specified date and time

ASSEMBLY RESTRICTED
If compromise of the information is likely to cause any of the following, a *RESTRICTED* marking is appropriate:

1. Cause substantial distress to individuals;
2. Breach proper undertakings to maintain the confidence of information provided by third parties;
3. Breach statutory restrictions on the disclosure of information;
4. Undermine the proper management of the NI Assembly and its operations;
5. Impede the effective development or operation of Assembly or Government policies
6. Make it more difficult to maintain the operational effectiveness or security of UK or allied forces.
7. Adversely affect diplomatic relations
8. Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies;
9. Disadvantage Assembly/Government in commercial or policy negotiations with others.
10. Prejudice the investigation or facilitate the commission of crime

ASSEMBLY CONFIDENTIAL
If compromise of the information is likely to cause any of the following a *CONFIDENTIAL* marking is appropriate:

1. Prejudice to individual security or liberty
2. Substantially undermine the financial viability of major organisations

3. Seriously impede the development or operation of major NI Assembly or government policies
4. Materially damage diplomatic relations, that is, cause formal protest or other sanctions.
5. Cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations.
6. Work substantially against national finances or economic and commercial interests.
7. Impede the investigation or facilitate the commission of serious crime.
8. Shut down or otherwise substantially disrupt significant national operations.

ASSEMBLY SECRET

If compromise of the information is likely to cause any of the following a *SECRET* marking is appropriate:

1. Raise international tension
2. Seriously damage relations with friendly legislators/governments
3. Threaten life directly, or seriously prejudice public order, or individual security liberty.
4. Cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations.
5. Cause substantial material damage to national finances or economic and commercial interests.

ASSEMBLY TOP SECRET

If compromise of the information is likely to cause any of the following a *TOP SECRET* marking is appropriate

1. Threaten directly the internal stability of the UK or friendly countries.
2. Lead directly to widespread loss of life.
3. Cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations.
4. Cause exceptionally grave damage to relations within friendly governments.
5. Cause severe long term damage to the UK economy.

ADDITIONAL CONSIDERATIONS

In exceptional circumstances, there may be occasions when the classification of information may have to be raised, for example if early disclosure would substantially undermine the effectiveness of the Northern Ireland Assembly, it may be necessary to classify the information 'ASSEMBLY RESTRICTED' 'ASSEMBLY CONFIDENTIAL' until the information is due for discussion/release. In such cases Information Asset Owners (IAOS) may want to consider applying classifications as listed above. IAOs should discuss this issue, if necessary, with the SIRO and if Committee related, the Chairperson.

Legal Advice

Legal Advice provided by the NIA Legal Services Office will be classified by Legal Services, in accordance with the policy.

All Legal Advice provided by the NIA Legal Services Office is privileged. **To protect privilege, the advice, or the substance of the advice provided, should not be disclosed, to any third party without contacting Legal Services.**

To maintain privilege, it is important that the advice is not shared, copied or disclosed beyond the individual(s) for whom it was intended. The issue of privilege should therefore be discussed to ensure all in receipt of advice are aware of the issue of privilege and handling arrangements.

Where the client is a Committee of the Assembly, privilege in the legal advice is vested in the entire Committee and not in any individual Committee Member (or Member of Committee staff). The disclosure of legal advice provided to a Committee without the approval of that Committee as a whole is a breach of the Committees privilege.

To maintain privilege, the issue of privilege should be discussed with Committee Members and copies of legal advice should be limited to those intended. For example, in order to maintain privilege and restrict legal advice to those for whom it was intended, legal advice is not included in the Electronic Committee Pack (ECP) as this information is shared wider than the Committee.

For advice regarding additional controls please see sections 6.3.11 and 6.3.12.

For further advice regarding storage (section 6.5), copying (section 6.4), transmission (section 6.7 & 6.8), disposal (section 7) and removal of information (section 8), please refer to the policy as controls will be applied depending on classification.

With the additional controls in place, the requirement for password protection on issue of legal advice is no longer required.

4. Application of Protective Markings

4.1 Exceptional Circumstances
There may be occasions when the classification of information may have to be raised, for example if early disclosure would substantially undermine the effectiveness of the Northern Ireland Assembly it may be necessary to classify the information 'ASSEMBLY RESTRICTED' 'ASSEMBLY CONFIDENTIAL' until the information is due for discussion/release. In such cases Information Asset Owners (IAOS) may want to consider applying classifications as listed above at Point 3. IAOs should discuss this issue, if necessary, with the SIRO and, if Committee related, the Committee Chair.

4.2 Only the originator, after consulting with the Information Asset Owner (IAO), can protectively mark an asset or change its protective marking, though holders of copies may challenge the level of protective marking applied.

4.3 On creation of information, consideration should be given to the protective marking, if any, to apply.

4.4 The protective marking should be centred at the top and bottom of every page. Media carrying protectively marked information should be clearly marked with the protective marking.

4.5 Assembly stamps will be available from the Stationery and Reprographics Office and should be requested by the Information Asset Owner (IAO)/SIRO in order to apply the relevant marking as required. This may be useful when applying protective marking to information which originated outside the NI Assembly.

4.6 When applying protective markings the creator should bear in mind that security controls can be costly; the higher the level of protective marking, the greater the cost of the protective controls it attracts. It is therefore important to take into account the level of access required and the implied costs of the protective controls that should be given when applying a specific protective marking.

4.7 Applying too high a protective marking to an asset can inhibit access, lead to unnecessary protective controls and impair the efficiency of the Assembly Secretariat's business. However, applying too low a protective marking can put information/assets at risk of compromise, since appropriate security controls may not be in place.

5. Controls for application of Protective Markings

The following controls are in place to ensure that assets are correctly marked.

5.1 Decisions regarding protective markings should be discussed with the SIRO / Information Asset Owner (IAO) based on the following: –

5.2 '**Assembly Restricted**'
This protective marking should be discussed and approved by the **Information Asset Owner (IAO)**.

5.3 **'Assembly Confidential'**
This protective marking should be discussed and approved by the **Information Asset Owner (IAO)**.

5.4 **'Assembly Secret', 'Assembly Top Secret'**
Use of high level protective markings must be approved by the **SIRO**.

5.5 Use of protective marking should be limited, for example, by encouraging the separation of the more sensitive information into appendices, so that the main body can be distributed more widely using less elaborate protective controls.

5.6 It should be emphasised that documents should not necessarily be given the same marking as those to which they are attached, refer to or are in response to.

5.7 Where possible, expiry limits should be set on markings so that protective controls do not apply for longer than necessary.

5.8 Where only parts of a document are classified, the relevant passages should be clearly marked by the creator. In such cases it may be practicable by omitting the classified passages to make up an unclassified version which can then be circulated in the normal way, in its unclassified form.

5.9 After consideration, one full copy of all classified papers should be retained and filed securely while the remainder should be shredded in accordance with disposal instructions, at Point 7, and in accordance with the NI Assembly Secretariat policy on record retention.

6. Procedures for handling of protectively marked data

6.1 Information with a protective marking should be kept secure and returned to appropriate furniture immediately after use. Such material should not be accessible to individuals unless they have permission to access. Protectively marked material must therefore not be left unattended at any time, both during the day and after working hours.

6.2 Information provided from Private Individuals or Bodies

6.2.1 Protective markings used by private individuals or bodies can vary greatly in their scope and application, and, for information classified up to and including ASSEMBLY CONFIDENTIAL and above, the Information Asset Owners should seek agreement with private individuals or bodies on the extent to which the documents should be circulated. In cases of doubt the SIRO should be consulted and agreement reached on the status of the documentation before circulation.

6.2.2 Consideration should be given to all material handled in the Assembly to ensure the appropriate protective marking is applied.

6.2.3 Information which has originated elsewhere must also be considered and an Assembly marking applied.

6.2.4 Where the originator does not want protectively marked material copied, a special handling instruction should be shown underneath the protective marking, for example:

Copy 1 of 8

ASSEMBLY CONFIDENTIAL

No copy to be taken without reference to and agreement of …….
(named individual)

6.2.5 Books and multi paged documents should show clearly the overall protective marking to reflect the highest component. Paper documents should be fastened securely and each page numbered. Where possible, the protective marking should be indicated at the beginning of each portion of the document to which it applies.

6.3 Registering, filing and distribution

The following controls should be applied when registering, filing and distributing protectively marked documents:

Mandatory Controls:

6.3.1 ASSEMBLY SECRET and ASSEMBLY TOP SECRET material must be registered and placed as soon as possible in serially numbered or otherwise uniquely identifiable files.

6.3.2 The content of files containing ASSEMBLY SECRET or ASSEMBLY TOP SECRET material should be serially numbered.

6.3.3 Copy numbers must be applied to material which is protectively marked ASSEMBLY CONFIDENTIAL or above. (For example, Copy 1 of 5). The asset should also bear the title of the originating office, a reference number and date of origin. Each page should be numbered in a separately identifiable series.

6.3.4 Material which is protectively marked CONFIDENTIAL or above should be made individually unique. Each single piece of documentation issued should have a unique reference that identifies to whom the report has been issued. Each paper is individually watermarked.

6.3.5 The movements of ASSEMBLY SECRET and ASSEMBLY TOP SECRET material, internally, incoming or outgoing to an organisation, and including disposal, must be recorded in a suitable register and maintained centrally by the Clerk/DG.

6.3.6 The movements of ASSEMBLY CONFIDENTIAL material, internally, incoming or outgoing to an organisation, and including disposal, must be recorded in a suitable register, maintained centrally by the Information Asset Owner (IAO) within the Directorate.

6.3.7 **All protectively marked material** should only be circulated to individuals who have permission to access.

6.3.8 Material which is protectively marked ASSEMBLY CONFIDENTIAL should be circulated on the basis that individuals do not discuss the contents in public meetings.

6.3.9 Each single piece of documentation marked ASSEMBLY CONFIDENTIAL or above, is individually watermarked. Where documents are provided in advance of discussion, for example for a committee meeting, the

documentation must be hand delivered directly to the relevant individuals, including Members, and to no one else. IAOs staff should maintain a record of who has received a copy and the date it was returned, if appropriate.

6.3.10 If an individual or Member is not available to take personal receipt of the document it should be retained by staff in a locked cabinet.

6.3.11 Additional controls: Where documents are not provided in advance of a meeting, there may be circumstances in which the Information Asset Owner determines, after consultation, if documents should be watermarked with individual names and only made available at the meeting and collected at the end.

6.3.12 Members could also be invited to come to a designated office to read draft reports and sensitive correspondence and where several items deemed sensitive are to be tabled for a meeting, the team reserves a reading room to provide Members enough time for full consideration of papers.

6.3.13 Material marked ASSEMBLY SECRET or ASSEMBLY TOP SECRET must be retained by the Clerk/DG in a locked safe.

6.4 Copying

The reproduction of protectively marked material, for example by photocopying, scanning or an electronic document forwarded by email should be kept to an absolute minimum and any copies handled in the same way as the original. Such material should not be copied to other staff as a matter of routine unless the business requires.

6.4.1 The originator may stipulate no copying or reproduction by annotating the document *"no copy is to be taken without reference to author*".

6.4.2 Some modern reprographic systems, including photocopiers, printers, scanners etc. have a facility to store copies of documents. Users should therefore exercise caution when using such equipment and should seek advice as follows:

- Advice regarding photocopiers should be sought from the Stationery and Reprographics Office.

- Advice regarding printers, scanners should be sought from IS Office.

The following controls should be applied when copying protectively marked material:

Mandatory Controls:

6.4.3 Copy numbers must be applied to material which is protectively marked ASSEMBLY CONFIDENTIAL or above. Where a recipient needs to make copies, the destination of copies made must be recorded on the original document.

Additional Controls:

6.4.4 Copying of protectively marked material should be kept to the minimum essential for the efficient conduct of business. Spare copies should be reviewed regularly for destruction.

6.4.5 Where the originator does not want protectively marked material copied, a special handling instruction should be shown underneath the protective marking, for example:

Copy 1 of 8 ASSEMBLY CONFIDENTIAL No copy to be taken without reference to and agreement of ….. .

6.4.6 Where the risk of compromise is high or when ASSEMBLY SECRET and ASSEMBLY TOP SECRET material is involved, reprographic systems, including photocopiers, printers, scanners etc. should be operated under proper supervision and the number of copies recorded in the register maintained by the Information Asset Owner (IAO) or Clerk/DG for SECRET/TOP SECRET documents.

Reprographic Systems - The following checks should be made after use:

6.4.7 Ensure to clear the machine of original and copy material after use

6.4.8 Users should ensure that any copies which have become trapped in the machine are identified and removed for secure disposal before requesting service support

Please refer to the following guidance on secure printing using the communal printers.

6.5 Storage

6.5.1 All protectively marked material should be tagged securely in appropriately marked registered files. The file should be marked to the level of the highest protectively marked document it contains.

6.5.2 When not in use material which is protectively marked should be kept locked as follows:

ASSEMBLY RESTRICTED
Locked in standard furniture

ASSEMBLY CONFIDENTIAL
Locked in approved security furniture

ASSEMBLY SECRET
Held by the Clerk/DG and locked in approved safe.

ASSEMBLY TOP SECRET
Held by the Clerk/DG and locked in approved safe.

6.6 Electronic Storage

Please note, the network is secure to hold information up to and including restricted. Please refer to the Policy for the use of IT Resources.
Secretariat Staff - Policy for the Use of IT Resources

For further advice regarding electronic storage please contact the IS Office.

6.6.1 Removable Storage Devices

Handling of removable storage devices must be in line with the classification of the information it contains. A limited number of devices will be approved for use. Each device will be registered to the particular user. Approved use of such devices should be sought from the Head of IS Office. When no longer required, devices should be returned to a central depository.

6.7 Transmission

6.7.1 Information marked **'ASSEMBLY RESTRICTED'.**
One new envelope should be used fully addressed with no protective marking. If delivery is by internal messenger/courier service the envelope should be

stamped ‘addressee only’. Material may be sent by in-house messenger service, Royal Mail letter post (recorded delivery and receipt obtained from the Post Office) and by approved courier service. The material should be contained in a plain non-identifiable envelope and should not be overfilled.

Information can be sent by ordinary fax if the recipient is on hand at the other machine to receive.

6.7.2 Information marked **‘ASSEMBLY CONFIDENTIAL’**
Information may be sent using Royal Mail letter post (recorded delivery and receipt obtained from the Post Office) in two plain non-identifiable envelopes and should not be overfilled. Information should NOT be sent by fax. Information may **NOT** be sent using the in-house messenger service (please see 6.3.9 for further information).

6.7.3 Information marked ‘**ASSEMBLY SECRET’** or ‘**ASSEMBLY TOP SECRET**’
Two new envelopes should be used both fully addressed with the protective mark and ‘to be opened only by addressee only’ on the inner one, with the individual’s name clearly marked on the inner envelope. Information must be hand delivered and signed for on receipt, both incoming and outgoing. Information should NOT be sent by fax.

6.8 Transmission by email

6.8.1 Material marked ‘ASSEMBLY RESTRICTED' may be sent by email to another Assembly Secretariat member of staff using their standard address in the format forename.surname@niassembly.gov.uk

6.8.2 Information classified ‘ASSEMBLY RESTRICTED’ and above should not be emailed to personal email accounts. Should staff be required to work at home, remote access to the Assembly’s IT network should be arranged. Further information can be obtained from the IS Office.

6.8.3 Use of encryption
Information marked ‘ASSEMBLY RESTRICTED’ or above must never be sent externally via email (i.e. to an email account other than an approved Assembly email address) unless approved encryption tools are used. All confidential material emailed to Members must be encrypted also. All passwords should be exchanged face-to-face or by telephone. Further information can be obtained from the IS Office.

6.8.4 Alternative arrangements for use of have been drawn up and approved by the Information Security Group for exchange of information with a limited number of organisations. Business areas must speak with the IS Office or Information Standards Office if they have any difficulty with the approved encryption

procedures. Alternative arrangements must be approved by the Information Security Group before enacted.

6.8.4 Disclosure of encryption passwords
Passwords used for encryption should be disclosed to the relevant person face to face or via telephone. Encryption passwords should be disclosed only to those who require access and should not be contained in or with the emailed document. Further information can be obtained from the IS Office.

6.8.5 A paragraph should be inserted in emails which contain restricted files, to advise the recipient that the content of the email are not to be disclosed to any other person and if the person is not the intended recipient, the email should be returned to the sender. Please note, this disclaimer is generated automatically for secretariat staff sending externally. It is not generated for Members and party support staff, or for secretariat staff sending internally. IS Office should be contacted for further details.

6.8.6 Use of Circulation Lists**.**
A check should be carried out to ensure both forename and surname is detailed on the list. Email addresses and attachments should also be checked before sending documents electronically.

6.9 Alternative encryption arrangements

Alternative arrangements have been approved by the Information Security Group for exchange of information with particular organisations. Such arrangements must be considered and agreed with the Information Security Group. Business areas must contact the IS Office if they have difficulty using encryption. Alternative arrangements for exchange of information are not permitted unless recommended by the IS Office and approved by the Information Security Group.

6.10 Requests for Personal / Sensitive Data - Verification Processes

Confirming a requester's identity

To avoid personal data about one individual being sent to another, either accidentally or as a result of deception, you need to be satisfied that you know the identity of the requester. You can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates (or a person authorised to make a Subject Access Request on their behalf).

The key point is that you must be reasonable about what you ask for. You should not request a lot more information if the identity of the person making the request is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.

The level of checks you should make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned.

Business Areas should consider what procedures they will adopt to suit their specific areas and staff should consult Information Asset Owners if they require any further advice.

7. Procedures for disposal of protectively marked information

7.1 All protectively marked material not due for permanent preservation, in accordance with the approved retention and disposal policy, should be destroyed securely at the appropriate time by means of cross-cut shredder. Cross-cut shredded waste can be placed in recycling bins. Further advice and information regarding availability of cross-cut shredder can be obtained from the Stationery and Reprographics Office.

On-site shredding is available for CONFIDENTIAL material. Please contact Sustainable Development for further details.

7. 2 Disposal of material classified ASSEMBLY CONFIDENTIAL or above must be overseen by a witness who should identify and log each item being destroyed, verify that each page of a multi-page document is present, noting the material disposed, date of disposal and those present. Registers of ASSEMBLY CONFIDENTIAL information are held centrally by the Information Asset Owner (IAO) within Directorates. A register of ASSEMBLY SECRET and ASSEMBLY TOP SECRET information is held centrally by the Clerk/DG. On-site shredding is available for CONFIDENTIAL material. Contact Sustainable Development for further details.

7.3 Protectively marked CDs, DVDs and other plastic material should be destroyed by shredding. For further advice please contact Sustainable Development.

7.4 Recycle bags should be used for material which is not protectively marked.

7.5 A record of the number of shredding, recycle sacks collected should be kept by Sustainable Development who are responsible for safeguarding and overseeing the destruction of protectively marked waste.

7.6 When the sacks are stored pending destruction, a record should be kept of the number received, the number subsequently destroyed or handed over for destruction to the waste company and receipts should be obtained. The record of sacks received, stored and destroyed should be checked regularly by Sustainable Development.

7.7 Shredding of material marked ‘Assembly Secret’ or ‘Assembly Top Secret’ should be CROSS CUT - supervised and removed from the shredding system immediately. Material that originated elsewhere (provided externally by an individual / department / organisation) and which has a protective marking of ASSEMBLY SECRET / ASSEMBLY TOP SECRET should be returned to the original owner or organisation for disposal and the register signed and updated to reflect this.

7.8 A record of the destruction of ASSEMBLY SECRET and ASSEMBLY TOP SECRET material must be logged in the register held by the Clerk/DG. This record, which should include the date and authorisation for destruction, must be kept for at least five years after the destruction date.

7.9 The destruction of ASSEMBLY SECRET and ASSEMBLY TOP SECRET material should be overseen by a witness who should:

- Identify each document being destroyed
- Verify each paper of a multi-page document is present
- Sign a certificate of destruction

7.10 Magnetic or optical media on which information marked 'ASSEMBLY RESTRICTED' has been recorded may be disposed of or reused provided an approved erasure package is used. Contact IS Office for further information.

7.11 Advice should be sought from IS Office when creating information marked 'ASSEMBLY CONFIDENTIAL', 'ASSEMBLY SECRET' or 'ASSEMBLY TOP SECRET'.

8.0 Removal of Protectively marked assets from official premises and Remote Access

8.1 Protectively marked assets removed from the office for meetings or approved home working should be carried securely, preferably, in a document holder/case and should remain in the possession of the individual at all times.

8.2 Protectively marked assets should not be worked on anywhere where the contents might be overlooked or otherwise noticed, and they should not be left unattended in any public place, such as restaurant, hotel, taxi or public transport vehicle.

8.3 The practice of taking material marked ASSEMBLY CONFIDENTIAL or above off the premises to be worked on at home or on the way to an official meeting, should be approved by SIRO/Information Asset Owner (IAO) and only permissible when the individual is briefed on the protective controls required and the risks to such assets can be effectively managed. Authority to do so must be sought on each occasion.

8.4 All protectively marked material should only be circulated to individuals who have permission to access. Material which is protectively marked ASSEMBLY CONFIDENTIAL should be circulated on the basis that individuals do not discuss the contents. This also applies to Members who should not discuss the content of protectively marked material outside closed meetings.

8.5 Only in exceptional circumstances would authority be given to the removal of ASSEMBLY TOP SECRET and ASSEMBLY SECRET material from the premises. Permission for such removal must be sought by the Clerk DG.

8.6 Remote Access

Information marked ASSEMBLY RESTRICTED or above must never be emailed to personal accounts. Should staff be required to work at home, remote access to the Assembly's IT network should be arranged. Please also refer to Section 6.8 - Transmission by email and use of encryption.

Please see attached link to instructions regarding remote access which are published on AssISt.

Further advice regarding remote access should be sought from the IS Office.

9. General Security

Ensure proactively marked items including storage devices are locked in appropriate standard and approved security furniture and the keys are secured before you leave the office.

Assembly staff should be aware that information gained as a result of their work should not be divulged to any unauthorised person. A breach of this policy will be considered under disciplinary procedures.

9.1 Clear Desk Policy

Please refer to Appendix A.

9.2 Security Containers (Key boxes/safes/ metal cabinets)

9.2.1 Keys which give access to security containers must be stored in wall mounted key boxes. Under no circumstances should the keys be removed from the office.

9.2.2 If a security key is damaged, or missing, or if a container holding protectively marked information has been tampered with, security should be informed immediately.

9.2.3 Spare keys for these types of containers should be held separately.

9.2.4 Managers should ensure that all staff understand their responsibility for securing cabinets and offices.

The following procedures should therefore be adopted by all staff:

9.2.5 Where appropriate, paper and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, including during working hours.

9.2.6 Sensitive or critical business information should be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.

9.2.7 Where necessary, incoming and outgoing mail points and unattended fax machines should be protected.

9.2.8 Personal computers and computer terminals and printers should not be left logged on when unattended and should be protected by key locks,

passwords or other controls when not in use. Any security policies in place should not be circumvented.

9.2.9 Sensitive or classified information, when printed, should be cleared from printers immediately.

9.3 IT Security

9.3.1 'Lock' your pc when unattended in the office (hold down ctrl, alt and delete keys)

9.3.2 “Shut down” your pc before you leave the office

9.3.3 Take care of IT equipment and storage devices and don't leave them lying around, or visible in your car. Please see AssISt for guidelines on use of IT resources.

9.3.4 Know the rules for handling protectively marked information.

9.3.5 Passwords must not be shared or written down for others to see. Please see password policy available on AssISt.

9.3.6 Secure printing (pin protected) should be applied when printing to a shared printer (Instructions available on Assist) and all information should be cleared from printers immediately.

9.3.7 For more information please refer to
Secretariat Staff - Policy for the Use of IT Resources

9.4 Access Management

9.4.1 The Information Asset Owner (IAO) should ensure that access to information is managed and up to date records are maintained of staff and privileges.

9.4.2 Staff movement and access system privileges should be managed in a timely manner and IS Office kept informed of changes to ensure file share permissions are reviewed and, where necessary, revised. Security Office should also be informed of any staff changes to ensure personal details of staff held are reviewed and disposed in accordance with retention and disposal policy.

9.4.3 The Information Asset Owner (IAO) should pay particular attention to

staff leaving the organisation. On receipt of resignation, access to sensitive information (ASSEMBLY RESTRICTED and above) should be removed and records updated accordingly.

9.4.4 HR will inform the IS Office, Security and the relevant Information Asset Owner (IAO), on an on-going basis, of any staff movement or change. (where the last day in the office is different from the last day of service, the Line Manager must advise the IAO, IS Office and Security Office).

9.4.5 Information Asset Owners should ensure HR are made aware of any further changes within business areas that may affect access management.

9.4.6 An email will issue from the Information Standards Officer quarterly, on behalf of the SIRO, requesting that all Information Asset Owners (IAOs) review access control for shared drives, databases etc. within their work area.

9.5 Spot Checks

9.5.1 The objective of spot checks is to ensure that the protective marking policy functions properly and is correctly implemented. It also acts as a deterrent against the improper removal of protectively marked documents, and will therefore be carried out without warning at frequent but irregular intervals.

9.5.2 Only a few documents need to be subject to a check at any one time.

9.5.3 Checks should be made without warning so that those responsible for such documents will not know when they might be asked to produce them.

9.5.4 A check should be made of ASSEMBLY TOP SECRET material at least 4 times a year and for ASSEMBLY SECRET material, at least twice a year.

9.5.5 Any breach of procedures may result in disciplinary action. Further details are contained in the NI Assembly Secretariat Terms and Conditions of Employment.

10. Descriptors

Commercial:	relating to the process or affairs of a commercial undertaking
Contracts:	concerning tenders under consideration and the terms of tenders accepted
Honours:	concerning the actual or potential award of an honour before its announcement
Legal – Privileged:	For use by Legal Services
Management:	concerning policy and planning affecting the interests of groups of staff
Personal:	material only to be seen by the person to whom it is addressed
Personnel:	containing references to named or identifiable staff or personal confidences entrusted by staff to management
Policy:	concerning proposals for new or changed policy before its publication
Regulatory:	material which has come into the possession of the Assembly in the course of carrying out its duties
Visits:	concerning advance details of visits by for example, Royalty, Ministers or very senior staff.

Appendix A

Clear Desk and Clear Screen Policy

Objective

The objective of the Clear Desk and Clear Screen Policy is to set guidelines which reduce the risk of a security breach and fraud; ensure compliance with Data Protection regulations; and reduce the risk of data loss or theft caused by information being left unattended on the premises.

Background

The main reasons we have introduced the policy are:-

- To reduce the threat of a security breach and information theft by ensuring that all work related information, excluding non-sensitive reference material and information which is in the public domain, is secure and locked away overnight or when leaving the office for a major part of the day. This may include laptops and detachable media such as, DVDs or memory sticks;
- To ensure compliance with Data Protection regulations by keeping personal data secure;
- To ensure that the NI Assembly Secretariat is taking corporate responsibility for information in its care.

The purpose of the policy is to have procedures and guidance in place to reduce the opportunity for security breaches and ensure compliance with the Data Protection Act by having controls in place to help advise staff in the handling of information within the organisation.

The Policy in Operation

- **A clear screen procedure**
  This should be adopted for information processing facilities in order to reduce the risks of unauthorised access, loss of, and damage to information during and outside normal working hours.

- **Lock personal computer (PC) when leaving the office**

  When leaving the office staff must ensure their PC is locked and information is not visible on the screen. To lock the PC, hold down the following keys on the keyboard – **ctrl**, **alt** and **delete**.

- **Staff must ensure they "shut down" their pc at the end of the working day.**

- **Storage Media**
  The policy includes removable storage media which may also contain information, this includes CDs, DVDs, memory sticks etc. Laptops and media of this type must also be cleared from desks and secured in appropriate furniture before going home or leaving the office for a major part of the day. Laptops must be cleared from the desk and locked in appropriate furniture.

- **Clear Desk**
  At the end of the working day or when leaving the office for a major part of the day, all staff are expected to clear their desk of the following:

  - all **work related papers and documents**;
  - **registered files**;
  - **removable storage media** (such as CDs, DVDs, memory sticks) which contains work related information;
  - work related **correspondence**;
  - **Protectively marked information**;
  - **work diaries** / **notebooks** which may contain work related information,
  - **contact details**, which are not in the public domain.

  Staff should also ensure that **notice boards and post-it notes** do not contain personal data.

  The policy excludes reference material and publicly available information.

  Desk furniture and filing cabinets are provided for storage purposes. Desk drawers and filing cabinets should be locked overnight and when leaving the office for a major part of the day.

  Keys should be secured before leaving the office and should be stored in wall mounted key boxes.

- **Material with a protective marking**
  Material with a protective marking should be kept secure and returned to appropriate furniture immediately after use. Such material should not be accessible to individuals unless they have permission to access. Protectively marked material must therefore not be left unattended on the desk at any time both during the day and after working hours.

- **Committee Packs**

Routine Committee packs will continue to be left in Members rooms or posted if requested.

Committee Packs containing confidential information/draft committee reports

Staff should ensure that Committee packs containing confidential information / draft committee reports are not left unattended in Members' offices at the time of distribution. Formal receipt must be acknowledged by Members. If a Member or their staff are not available to take receipt of the Committee pack, it should be held securely in the Committee Office until arrangements are in place for receipt.

- **Reprographic Systems**

The following checks should be made after use and before leaving the office at the end of the working day or for a major part of the day:

- Ensure to clear the machine of original and copy material after use.
- Ensure that any copies which have become trapped in the machine are identified and removed for secure disposal before requesting service support.

Adherence to the Policy

It is the personal responsibility of each member of staff to adhere to this policy. Compliance with the policy is the responsibility of line management and Heads of Business.

A breach of this policy will be considered under disciplinary procedures.

Appendix B

Duties of Information Asset Owners (IAOs)

- Ensure staff are aware of the Protective marking policy and procedures, including the policy for clear desk and clear screen.

- Meet on a regular basis with the SIRO to ensure consistency of approach throughout the NI Assembly.

- Dissemination and monitoring of the policy, type and use of information held in each directorate and responsibility for monitoring use of assets including hardware and software.

- HR Office will advise the relevant IAO, IS Office and Security Office, on an on-going basis, of staff movement or change. The IAO should ensure that access privileges to information are managed on a timely basis and up to date records are maintained of staff and access rights to, for example shared drives, databases etc.

- The Information Asset Owner should ensure HR is informed of any further changes within the business area that may affect access management. HR will ensure that the IS Office and Security Office are kept informed of all changes to ensure file share permissions are reviewed and, where necessary, revised.

- On a quarterly basis the Information Standards Officer, on behalf of the SIRO, will request all Information Asset Owners to review access control within their business area. IAOs will be required to confirm when this review is complete.

In compliance with the Protective Marking Policy:

- Ensure controls in place for the application of protective markings;

- Provide advice to staff on protective marking, up to and including 'Assembly Confidential', as necessary;

- Review protective markings up to and including 'Assembly Confidential' as required. If necessary discuss with the originator and change as appropriate;

- Ensure the following procedures are in place:

  - Handling of protectively marked material
  - Registering and filing protectively marked material
  - Copy, storage, transmission and disposal

- Maintain and update a register for all Assembly Confidential material held within the business area;

- Consider and approve, as appropriate, staff removal of Assembly Confidential material from the premises to be worked on at home or on the way to an official meeting. Approval must be considered for each occasion.

- Provide assistance to the SIRO as requested.

Appendix C

A list of Information Asset Owners can be accessed here