LEGISLATIVE ASSEMBLY

FOR THE AUSTRALIAN CAPITAL TERRITORY

Office of the Legislative Assembly – March 2021

OLARIS	21/001634
Version/Approved	1 March 2021
Review	March 2024

Information and Communications Technology Security Policy and Framework

Contents

Introduction

1. This paper establishes a framework to ensure that the Legislative Assembly for the Australian Capital Territory (the Assembly) operates in an effective information and communications technology (ICT) security environment. It recognises the position that the Assembly has adopted in maintaining a distinct separation from the Executive, while taking advantage of the opportunities and efficiencies that linking to the ACT Government's network and using a common ICT service provider can offer.

2. The Assembly's ICT services will be guided by the policies that have been developed by Shared Services Information and Communication Technology (SSICT) on behalf of the ACT Government, particularly where these relate specifically to the services that SSICT provides to the Assembly under the memorandum of understanding (MOU) which has been agreed to by both organisations. However, the Assembly will develop specific policies, guidelines and procedures wherever necessary in order to ensure the security of its electronic information.

Policy framework hierarchy

3. This ICT security policy and framework was developed with reference to the:

    (a) whole of government security standards and policies for physical and ICT systems developed by SSICT as outlined in paragraph 2

    (b) threat and risk assessments for the Assembly's ICT systems identified in the risk register developed by the Director Officer of the Clerk in consultation with the Director Information and Digital Services

    (c) Australian/New Zealand Standard - Information technology — Security techniques — Code of practice for information security management (AS/NZS ISO/IEC 27002).

4. The policy is supported by other policies, guidelines and fact sheets developed by the Office of the Legislative Assembly (OLA) to provide specific advice on issues and supplement policy statements.

5. This policy should be read in conjunction with the ACT Government's Cyber Security Policy and other related policy documents (see list at the end of attachment A). Assembly staff, which includes staff of

non-executive members and OLA staff, must comply with both the whole of government and the Assembly's policies.

6. The cyber security roles and responsibilities of both SSICT and OLA are defined in the Assembly's Cyber Security Overview.

Overview

7. The Assembly's ICT systems are configured in a separate organisational unit on the ACT Government network (ACTGOV). This reflects the findings of the Standing Committee on Administration and Procedure's Inquiry into the role of InTACT as the Legislative Assembly ICT service provider (18 November 2003 —Report No 4).

8. The committee' recommended, among other things, that:

   (a) the Secretariat (now OLA) should assume responsibility for ICT user account creation and management (both login and email accounts)

   (b) a MOU should be developed between the ACT Executive and the Speaker of the Assembly and a SLA should be developed and implemented between InTACT (now SSICT) and the Assembly, and

   (c) OLA should develop and implement an ICT security policy and associated procedures for all staff, outlining responsibilities and the broader ICT security arrangements and procedures.

9. The Government response to the report was tabled In the Assembly on 4 March 2004 and was generally supportive of the committee's findings. The recommendations have now been implemented and this policy and framework is a consolidation of ICT security policies and guidelines which have been in place since that time.

10. A change in SSICT's business model has since replaced the need for an SLA with a Catalogue of Services.

Policy statement

11. OLA is committed to protecting the availability, confidentiality and integrity of the Assembly's electronic information. To ensure that this commitment is effectively implemented, OLA will:

    (a) define what constitutes acceptable and unacceptable use of its ICT systems for all users

    (b) implement specific guidelines and procedures relating to access control, account creation and management, remote use of the Assembly's ICT systems and other matters relevant to the configuration of the Assembly's ICT environment as a separate organisational unit

    (c) adhere to whole of government policies and practices relating to information classification, asset management and other matters where these are sufficient to protect the Assembly's interests, and

    (d) ensure that all users of the Assembly's ICT systems are aware of the requirements for, and their responsibilities in, protecting the Assembly's electronic information.

Information and communications technology security framework

Matters covered

12. A primary responsibility for OLA is to ensure that all users of the Assembly's ICT systems are aware of and comply with the Assembly's Policy on the acceptable use and management of information and communications technology and electronic information (Attachment A). Each user must read the policy and non-executive members' staff and OLA staff must sign the Assembly's "acceptable use declaration" at the end of this document. Users must obtain, through their employing member or director, approval from Business Support Branch, Manager Human Resources and Entitlements, before they can gain access to the Assembly's ICT systems.

13. The acceptable use policy also sets out the responsibilities of each user in protecting electronic information by taking steps to prevent unauthorised access to their login and email accounts and by storing electronic information appropriately. The policy is the principal source of guidance for Assembly ICT users and is included at attachment A.

14. All other policy documents relating to the security of the Assembly's ICT network and other electronic resources are set out at the end of attachment A. These policies will be regularly reviewed to ensure that they meet the continuing requirements of the Assembly. Where whole of government policies and procedures are found to be not applicable to or inappropriate for the Assembly, OLA will adopt policies and procedures which specifically address the Assembly's needs. OLA has to date developed its own policies, procedures or guidelines in the critical areas of risk management, change management, electronic information management, ICT asset management and use of Assembly supplied devices and applications during overseas travel. These are discussed in more detail in the following sections.

Risk management

15. OLA has developed a risk management policy framework to manage and control the internal or external threats confronting its operations which have a potential to jeopardise the achievement of its key objectives. Global risk assessments are undertaken each two years in accordance with the policy.

16. The Assembly, in conjunction with SSICT, will respond to newly identified threats by updating its business continuity plan.

17. OLA directors will undertake a risk assessment, including strategies to effectively control all identified risks, before seeking approval for a new business application.

18. For further information on risk management and business continuity, contact the Director Office of the Clerk.

Change management

19. The Assembly's ICT systems are either hosted on, or accessed via, the ACT Government’s standard operating environment which is locked down to prevent unauthorised access to its electronic information and disruption to ICT services.

20. All new hardware and software installations need to be approved by the Assembly IT Manager and must be compatible with SSICT's infrastructure and security policies. Large or complex system installations may also require SSICT change control procedures and/or project management services.

21. Business system owners must comply with appropriate legislative and auditing requirements.

22. For more information refer to the Assembly ICT fact sheet – Change Management.

Use of Assembly supplied devices and applications during overseas travel

23. Assembly ICT users planning to travel overseas for personal or work purposes and intending to take a private or corporate mobile device that will be used to gain remote access to the Assembly ICT network must comply with the requirements specified in the Assembly ICT Security Policy – use of Assembly supplied devices and applications during overseas travel.

24. Users must notify the Assembly IT Manager of their itinerary (including the dates and countries being visited) at least two weeks prior to travel so that advice can be sought from the Justice and Community Safety Directorate who will advise on the general risk level associated with the countries being visited and the measures that must be taken with regards to use of mobile devices and services within those countries.

Electronic Information management

Backup and restoration of electronic data

25. There is no specific backup and restore arrangement in place for Assembly's electronic data which mandates separation of its backup data from the rest of the ACT Government. This is not considered to be necessary as only members of the SSICT Storage and Backup team have access to backup data. As acknowledged in the MOU between the Speaker of the Legislative Assembly and the Executive Minister responsible for SSICT, all these staff have appropriate security clearances.

26. SSICT staff will not access the Assembly's information without written authorisation from the Assembly IT Manager. The Assembly IT Manager will monitor requests for restoration of backup data to make sure that restoration is managed appropriately.

27. For more information see the Assembly ICT fact sheet – backup, retention and restoration procedures.

Virus protection

28. SSICT adopts controls to protect electronic information stored on the Assembly ICT network against malicious code.

29. For further information see the ACT Government's Cyber Security Policy.

ICT asset management

30. Responsibility for the security of the ICT assets contained within the Legislative Assembly precinct rests with the Business Support Branch. The management of the Assembly's ICT assets within the precinct, including their issue, redeployment and disposal rests with the Assembly IT Manager who will ensure that any data saved on these assets is removed prior to redeployment or disposal. SSICT is responsible for the management of ICT infrastructure equipment in the Legislative Assembly and North building communications rooms.

31. For more information see the Assembly ICT fact sheet – Asset Management.

Information security awareness and training

32. All new Assembly ICT users are required to read this policy and sign the attached Policy on the acceptable use and management of information and communications technology and electronic information.

33. Non-Assembly staff (including contractors, consultants, volunteers, interns and students) who are authorised to access the Assembly's ICT systems will also be required to read this policy and sign the attached acceptable use policy.

34. Assembly ICT staff will provide new users with an ICT induction on their first login to the Assembly ICT network which will include familiarisation training on the Assembly's ICT systems.

35. Information and communications technology security awareness information is also included in new starters seminars held periodically and new members seminars held at the commencement of each new Assembly.

36. New and existing users will be provided with ICT security awareness information on topics such as responsibilities, potential security risks and countermeasures.

ICT security compliance

37. OLA's Internal Audit Committee will periodically incorporate ICT security policy and compliance audits into its audit program, as part of its regular review of OLA activities.

Assignment of responsibilities

The Speaker

38. The Speaker has overall responsibility for the administration of services, including ICT services, provided to non-executive members, their staff and OLA staff.

The Clerk

39. The Clerk is responsible to the Speaker for ICT security throughout the Assembly and is the owner of the ICT security policy and framework. The Clerk is also responsible for establishing a security-aware culture and for providing adequate resources to ensure the maintenance of a secure ICT environment.

Non-executive members

40. Non-executive members should be aware of the Assembly's ICT security policy and framework and their obligations under the Members' Code of Conduct. Members are individually responsible for the safekeeping of ICT assets issued to them and for all activity on their user accounts.

Non-executive members' staff

41. Non-executive members' staff are individually responsible for the safekeeping of ICT assets issued to them and for all activity on their user accounts. They must be aware of and comply with the Assembly's ICT security policy and framework. They should also be aware that relevant criminal, secrecy or privacy legislation may apply in their use or disclosure of official information. Breaches of such legislation may result in criminal and/or other disciplinary action.

OLA staff

42. OLA staff are individually responsible for the safekeeping of ICT assets issued to them and for all activity on their user accounts. They must be aware of and comply with the Assembly's ICT security policy and framework. They should also be aware that relevant criminal, secrecy or privacy legislation may apply in their use or disclosure of official information. Breaches of such legislation may result in criminal and/or other disciplinary action under the Public Sector Management Act.

OLA directors

43. OLA directors must ensure that staff are fully aware of the Assembly's ICT security policy and framework. They will monitor compliance with the policy and associated guidelines and procedures and report any suspected breaches to the Director Information and Digital Services.

44. Directors contemplating the development of a new business system must undertake a risk assessment, including strategies to effectively control all identified risks, before seeking approval for the new system. Directors who are business system owners are responsible for complying with appropriate legislative and auditing requirements.

Director Information and Digital Services

45. The Director Information and Digital Services is responsible for all matters relating to ICT security, including the development of policies, guidelines and procedures and ICT administration. The director will work closely with the Assembly IT Manager and OLA directors to ensure the implementation and maintenance of an appropriate ICT security policy and framework, including monitoring and responding to ICT security incidents occurring within the Assembly's organisational unit, and facilitating training and awareness of ICT security issues for Assembly staff.

46. The Director Information and Digital Services is also responsible for managing and controlling ICT security risks included in the OLA's Risk Management Policy and Framework.

Director Office of the Clerk

47. The Director Office of the Clerk is responsible for the overall planning and policy development associated with risk management, including conducting regular global risk assessments, and will work with the Director Information and Digital Services in regularly assessing ICT security risks.

Assembly IT Manager

48. The Assembly IT Manager is the primary contact and has day to day responsibility for all matters relating to ICT security within the Assembly.

49. The Assembly IT Manager is responsible for information security awareness and training.

SSICT staff

50. SSICT is the Assembly's ICT service provider and is responsible for the supply, management and maintenance of the ICT infrastructure, and for maintaining the availability and security of the Assembly's production and backup data. SSICT staff must:

    (a) be aware of and comply with the Assembly's ICT security policy and framework

    (b) comply with the provisions of the MOU between the Speaker of the Legislative Assembly and Executive Minister responsible for SSICT

    (c) implement whole of government ICT security measures and controls, including threat and risk assessments for new and existing ICT infrastructure services, on the Assembly ICT network as appropriate

    (d) provide advice on ICT security issues when requested by the Assembly

    (e) respond within the appropriate timeframe in the event of a security incident affecting the whole of government ICT infrastructure and associated services, and

    (f) access the Assembly's backup data only on written authorisation from the Assembly IT Manager.

Internal Audit Committee

51. OLA's Internal Audit Committee has an oversight role in relation to compliance with ICT security requirements.

Breaches of the ICT security policy

52. Any OLA staff member, staff of non-executive members of the Assembly or non-Assembly staff including contractors, consultants, volunteers, interns, and students who becomes aware of a suspected or actual breach of this policy should report it to a supervisor, their member or the Assembly IT Manager.

53. Access to the Assembly's ICT resources may be denied to any person found to be in breach of this policy and anyone suspected of breaching this policy may also have their access suspended temporarily, in any case, OLA's formal disciplinary process may apply.

Tom Duncan
Clerk of the Assembly

Attachment A

LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

Assembly ICT Policy —acceptable use and management of information and communications technology and electronic information

Introduction

1. Staff who are employed or engaged by the Office of the Legislative Assembly (OLA) or by a non-executive member of the Legislative Assembly have access to a range of resources and technologies in the workplace to enable them to carry out their official duties. Each user must accept responsibility for protecting the Assembly's electronic information, preventing unauthorised access to that information, and making acceptable use of information and communications technology (ICT).

Information security

2. Information security is the protection of information from a wide range of threats to ensure:
    (a) confidentiality of personal and official information
    (b) integrity, accuracy and completeness of data
    (c) business continuity through the availability of a fully functioning system and its components, and
    (d) efficient and appropriate use of resources.
3. Information security is achieved through implementing a suitable set of controls including policies, processes, procedures, organisational structures and software and hardware functions.

Application

4. The policy applies to the Legislative Assembly’s information and communications technology (ICT) network which forms part of the ACT Government ICT wide area network infrastructure. This environment consists of a range of ICT products and services which is locked down to form a standard operating environment (SOE) that can be accessed by ACT Government and Assembly IT users. This policy shall use the term “Assembly ICT network” to reflect the standard operating environment available for use by Assembly ICT users.
5. This policy applies to all Assembly staff when they are using the Assembly's ICT network. Assembly staff includes OLA staff and staff of non-executive members of the Assembly. This policy also applies to non-Assembly staff including contractors, consultants, volunteers, interns, and students. This policy shall use the term "user" that includes all Assembly and non-Assembly staff who are using Assembly ICT network.

Access to the Assembly ICT network

6. Access to the Assembly ICT network is subject to the following conditions:

    (a) users must, through their employing member or director, obtain the approval of the Business Support Branch, Manager Human Resources and Entitlements

    (b) users must read this policy and sign the "acceptable use declaration"

    (c) users must participate in an IT induction on their first login to the Assembly IT network

    (d) authorised users must use a computer that is configured in accordance with the SSICT standard operating environment or use a SSICT remote access service, and

    (e) users are responsible for the safekeeping of any ICT device issued to them.

7. Authorised users of the Assembly's ICT network must:

    (a) be aware of their responsibilities and what they are authorised to do, and

    (b) have an expectation of detection if they abuse their privileges.

8. Any resources allocated to the user including ICT equipment, software or services must be returned to OLA before the user's termination date. This also applies to any user who ceases to be employed by a member even though they may sign a volunteer agreement.

Private use

9. Whilst it is accepted that there will be incidental private use of the Assembly's technology and resources, any private use must be kept to a minimum. Staff are expected to apply sound judgment and common-sense in these matters and take reasonable steps to eliminate inappropriate practices from the workplace.

Unacceptable use

10. The use of the Assembly's ICT resources to intentionally view, display or disseminate abusive, aggressive or deliberately anti-social material (including pornographic or sexually or racially harassing material) is unacceptable, unless this is undertaken as part of the official duties performed by a staff member. If users are in doubt about whether their use of Assembly information technology to view, display or disseminate such material would be in breach of this policy, they should consult their employing member, their Director, or the Assembly IT Manager.

11. It is inappropriate for a staff member to use Assembly ICT resources to:

    (a) breach any relevant laws including, but not limited to, the Copyright Act 1968, the Parliamentary Privileges Act 1987, the Legislative Assembly (Broadcasting) Act 2001

    (b) interfere with or disrupt other ICT users, services or equipment in the Assembly and ACT Government ICT environments

    (c) assist members with election campaigning, other party-political activities or private purposes not related to the discharge of their duties as elected representatives (refer to the Members' Guide— Chapter 18— Office Accommodation and Facilities), and

    (d) access or retain information which is intended for another person.

12. To help prevent staff viewing inappropriate material, either intentionally or unintentionally, and to guard against malicious damage, the Assembly uses the following services from SSICT, including:

    (a) Internet content filtering which applies to all OLA staff and staff of non-executive members. This service will either block access to inappropriate sites or warn users that they are about to enter an inappropriate site. For more information see the Assembly ICT fact sheet – Internet content filtering

    (b) Email SPAM filtering is enabled on all office email accounts. This service enables the user to filter. SPAM and other undesirable emails before they reach the mailbox. For more information see SSICT's Email spam filtering fact sheet

    (c) Virus protection which is mandatory on all Assembly ICT network connected computers and laptops, and on email and internet infrastructure equipment managed by SSICT. For more information see SSICT's Computer virus protection fact sheet.

System classification

13. The Assembly's ICT network is classified as PROTECTED and must only be used to write, print, store or transmit Information up to this level. A description of the types of information that falls into this category is included in the ACT Government's ICT Security Policy.

Electronic information management

Protecting electronic information

14. Assembly ICT users have an obligation to protect the confidentiality, integrity and availability of the electronic information they have access to in the Assembly's ICT network and to maintain the physical security of the resources and technology they use to gain access to information,

15. All electronic information which is stored or transmitted on the Assembly's ICT network becomes part of the Assembly's or the employing member's records and may be accessed by the Clerk or employing members in some circumstances. This includes information stored in a user's personal electronic storage area (H: drive). Employees should avoid using the Assembly's ICT network to store and transmit sensitive personal information or other non-work-related material.

16. If users receive or gain access to electronic information not intended for them, they have an obligation to report this situation to the Clerk of the Legislative Assembly, their MLA or Assembly ICT staff. If users receive material which has been sent inadvertently, it may be appropriate for them to notify the sender in the first instance.

17. The Clerk may approve access to logs of a user's activities on the Assembly's ICT network at any time where unacceptable use is suspected. Such access will be granted only to authorised persons. An authorised person is the Clerk, Assembly ICT staff, or a member of the SSICT cyber security team.

Storing electronic information

18. Assembly ICT users are responsible for storing electronic information in a way that allows it to be accessed efficiently and appropriately. Generally, unless otherwise instructed by a staff member's employing member or Director, all electronic Information should be stored as follows:

    (a) work-related documents should be saved on the Assembly ICT network, in the office G: drive, so that they can be shared with other staff in the office

(b) personal documents should be saved on the Assembly ICT network in the user's personal H: drive to prevent access by other staff

(c) any non-work related documents or files should not be stored on the Assembly ICT network, these should be stored on the user's computer C: drive or on a portable storage device such as an external hard drive or thumb drive, or CD/DVD

(d) users should not use the Assembly ICT network (G: and H: drives) for storing games, photos, music, videos or use the facility to backup information saved elsewhere, and

(e) users should not save important or sensitive documents on their computer C: drive as this information is not backed up and may be accessible to other staff who use the computer.

Portable storage devices

19. Portable storage devices may be connected to and used on Assembly IT network computers (e.g. USB hard drives and thumb drives, DVDs and CDs), however, these devices should not be used to store official information. The same applies to hard drives on other portable mobile devices such as laptops, tablets and mobile phones.

20. Storing sensitive records, information and data on portable storage devices is discouraged and should only be done on occasions where there is a short-term working need. If a user needs to store content temporarily for working purposes, they are responsible for its safekeeping.

21. All portable storage devices must be kept securely at all times to protect them and the information contained on them from loss or theft. For more information about information security see the ACT Government's Encryption Policy and Standards.

User login account

22. Assembly ICT users are responsible for the activities conducted within their personal login accounts. They should take the following precautions to prevent unauthorised access to those accounts:

    (a) choose a password that complies with the standards outlined in the ACT Government's Password Policy and Password Standard documents

    (b) not divulge their password or write it down where someone can find it

    (c) not use another staff member's login account and not allow other staff members to use theirs

    (d) log out of the Assembly's ICT network when they have finished work for the day

    (e) lock their computer desktop before leaving it unattended for any length of time, and

    (f) password protect their computer screen saver and set it to activate after several minutes of computer inactivity.

User email account

23. Assembly ICT users are responsible for the activities conducted within their personal email accounts and for the activities conducted by other individuals they delegate access to. To prevent unauthorised access to their email accounts, users should check their mailbox delegations regularly and ensure that only trusted individuals have access to their mailbox.

24. When sending and receiving emails:

(a) Users may use Assembly "all staff" distribution lists to send emails regarding work related matters (these are prefixed with #LA in the mail directory)

(b) Users may not use ACT Government distribution lists unless they have permission to do so from the relevant business owner or directorate

(c) Users must be wary of emails they receive from unknown sources as these may contain inappropriate material or virus-infected attachments (exercise caution when acting on emails seeking personal or confidential information)

(d) Users will not be able to send emails with file attachments greater than twenty-five megabytes which is the email system limitation, and

(e) Users must not access other email accounts unless they have permission to do so from the account owner.

Electronic external communications

25. Assembly staff who are using information and communications technology to communicate with people outside the organisation are expected to maintain the same high standards of conduct and behaviour online as would be expected elsewhere.

26. Assembly ICT users should be aware that the use of social media and other online activities has the potential to open opportunities for social engineering and for external parties to gain unauthorised access to confidential or sensitive information.

27. Social engineering, "the act of manipulating people into performing actions or divulging confidential information"[1], predates social media and the internet. With a little knowledge and information, a good social engineer can gain access to confidential or personal information with relative ease,

28. Social media sites make it very easy to share information with others. While this convenience is their selling point, it means that users need to be more careful than usual when using these sites:

    (a) Users should check their account and privacy settings – users need to be aware of who can access their postings before they post them. Users should also check that they are not revealing more personal information about themselves than is necessary

    (b) Users should review their posts before adding them to a site to ensure they have not revealed more than they should

    (c) Users should consider any 'Friends' requests carefully - especially from people they do not know. User should not reveal more information than is necessary or end up with less than professional updates from others on the user's professional profile.

29. If a user suspects that an attempt to elicit sensitive work-related information has been made (through online activities either at home or at work), they should notify the Clerk or the Assembly IT Manager.

Remote access

30. Assembly ICT users must have the approval of their employing member or director and the Assembly IT Manager to gain remote access to the Assembly's ICT network. Authorised users must use an approved SSICT remote access service which the Assembly IT Manager will arrange. Remote access via any other means is unauthorised. For more information see the Assembly ICT fact sheet – Remote Access Services.

[1] Wikipedia entry on Social Engineering: http://en.wikipedia.ora/wiki/Social engineering (security)

31. Remote access users should take the following precautions to prevent unauthorised access to their login account:

    (a) users who have been given a security token must protect it from damage and unauthorised access

    (b) users must lock their computer and de-activate their remote access session before leaving the computer unattended

    (c) users must ensure that the computer they are using to gain remote access has the latest security updates and virus protection

    (d) users should, when using internet cafes or wireless "hotspots", seek advice on whether the service provider has network security and virus protection and should not use services that do not have this protection.

Microsoft Office 365

32. SSICT manages the ACT Government software licensing agreement for Microsoft (MS) Office 365 which enables Assembly IT users to access certain MS Office products via their office based computer and online via the Office.com website using any computer or mobile device with an internet connection. User can also access their office mailbox via the Office.com website. The Assembly IT Manager can arrange for the purchase and installation of additional products when required.

ICT equipment installations

33. The Assembly IT Manager is responsible to the installation of ICT equipment (e.g. telephones, laptops, computers and print devices) on the Assembly ICT network. Generally, only Assembly provided ICT equipment, acquired through SSICT, will be connected to the Assembly ICT network as this equipment has been tested and approved for use on the Assembly IT network and is installed with a standard operating environment that is secure and supported by SSICT.

34. The Assembly IT Manager may approve the local installation of peripheral devices (e.g. label printers) on Assembly desktop computers (PC and laptops) which will be subject to certain conditions associated with security risk assessments, compatibility and cost.

Bring your own devices (BYOD)

35. Privately owned computers (PC and laptops) and mobiles devices (tablets and mobile phones) will not be connected directly into the Assembly ICT network due to the security risks, compatibility issues and costs involved.

36. Privately owned computers and may be used to connect wirelessly to the Assembly IT network, via:

    (a) the SSICT approved wireless network (e.g. ONE and ACTGOV public)

    (b) a SSICT approved mobile application (for tablets and mobile phones only), or

    (c) SSICT remote access service (for PCs, e.g. CITRIX).

37. SSICT and Assembly ICT staff will not provide support for private devices, however, they may assist the owner of the device to connect to a SSICT approved wireless network or to setup a SSICT approved remote access service.

38. The owner of a private device is responsible for the backup, maintenance, support and cost of their device. They must also accept full responsibility for any issues and costs that may arise as a result of any installation and/or connection to the Assembly ICT network.

39. Assembly IT users must not use their private devices accessing corporate information or business systems without written approval from their member or director.

Software installations

40. The installation of software on Assembly computers and the Assembly ICT network is subject to Assembly IT Manager approval which is based on the following conditions:

    (a) all software installations must be compatible with the Assembly IT network standard operating environment (SOE)

    (b) all software must be appropriately licensed. The Assembly IT manager will arrange for the purchase and installation of new software through SSICT

    (c) for privately purchased software, the Assembly IT manager will require a proof of purchase and installation terms and conditions. However, due to the ACT Government's software licensing agreement with Microsoft and Adobe, it may not be possible to install certain products unless they are purchased through SSICT

    (d) software that has not been tested on the Assembly IT network will be subject to SSICT change control processes, which depending on the complexity of the installation may incur additional costs for an ICT security risk assessment, software packaging and user acceptance testing, and

    (e) software deemed by the SSICT security team to pose an unacceptable risk to the security of the Assembly IT network will not be installed.

COVID-19 pandemic response

41. Wherever possible, Assembly ICT staff will provide support and changes remotely rather than in person. Where an in-person visit is required, a 1.5 metre distancing between all persons is to be observed. Hand sanitiser must be used before and after visits. Assembly IT users should ensure that ICT equipment is cleaned after use. For more information see COVID-19 response page on the OLA intranet.

More information

42. For more information about this policy, please contact the Assembly IT Manager.

43. Further information and documents can be found at the following links:

Shared Services ICT documents

SSICT ICT Policies, Guidelines, Standards and Fact sheets:
https://actss.service-now.com/sharedservices/?id=knwl_category&kb_category=7d876add150a47c0750353a7d14f17a5

Acceptable Use Policy
https://actss.service-now.com/sys_attachment.do?sys_id=366fc638dbde88d094034cf38a961942&view=true

ACT Government Cyber Security Policy
https://actss.service-now.com/sys_attachment.do?sys_id=0cb3bbcf1b8d2450dcfd20a13d4bcb0d&view=true

Password Standard
https://actss.service-now.com/sys_attachment.do?sys_id=f4361a5bdb11f788ac3eabf34a96198b&view=true

Email Spam Filtering
https://actss.service-now.com/sharedservices?id=knwl_article&sys_id=3090d232c5c9b2c05c7ea0e403683706

Complete Virus Protection
https://actss.service-now.com/sharedservices?id=knwl_article&sys_id=03d81500b05e9f407503f6c199982800

Encryption Standard
https://actss.service-now.com/sys_attachment.do?sys_id=b2425c43db738054cb8a6a1505961938&view=true

Office of the Legislative Assembly documents

Cyber Security Overview:
https://actgovernment.sharepoint.com/sites/Intranet-OLA/Documents/OLA%20Cyber%20Security%20Overview.pdf

ICT Security Policy and Framework, policies, guidelines and fact sheets:
https://actgovernment.sharepoint.com/sites/Intranet-OLA/SitePages/Information%20and%20Digital%20Services.aspx

Assembly ICT fact sheet - Remote Access Services:
https://actgovernment.sharepoint.com/sites/Intranet-OLA/Documents/RemoteAccessServicesFactSheet.pdf

Assembly ICT fact sheet - Asset Management
https://actgovernment.sharepoint.com/sites/Intranet-OLA/Documents/IT_Asset_Management_TT_022_HCL_1405_1705.pdf

Assembly ICT factsheet - Change Management:
https://actgovernment.sharepoint.com/sites/Intranet-OLA/Documents/IT_Change_Management_TT_024_HCL_1405_1705.pdf

Assembly ICT factsheet - Backup, Retention and Restoration:
https://actgovernment.sharepoint.com/sites/Intranet-OLA/Documents/IT_Backup,_Retention_and_Restoration_TT_023_HCL_1405_1705.pdf

Assembly ICT Security Policy – use of Assembly supplied devices and applications during overseas travel:
https://actgovernment.sharepoint.com/:w:/r/sites/Intranet-OLA/Documents/ICT%20Security%20Policy%20-%20Use%20of%20Assembly%20supplied%20devices%20and%20applications%20during%20overseas%20travel.DOCX?d=wbe817342fbf149e6be3183876318f1a1&csf=1&web=1&e=gRn3hY

ACCEPTABLE USE DECLARATION

I, _____, declare that:

(Write full name in block letters using ink)

a) I have read and understood the Legislative Assembly's Policy on the acceptable use and management of electronic information and information technology dated January 2021
b) I agree to abide by the requirements for access to and use of these resources
c) if I become aware of a suspected or actual breach of this policy I will report it to the Clerk or the Assembly IT Manager.

Signature: _____

Office: _____

Date: _____