VicRoads IT&T Security Policies

September 2004

VicRoads IT&T Security Policies

PURPOSE

The purpose of this document is to Increase awareness and understanding by staff, external customers and IT&T service providers of VicRoads security requirements when using or supplying computer facilities and services.

Information is of strategic importance to VicRoads, for a variety of purposes, including servicing customers, planning, controlling, reporting and internal decision making related to day-to-day operations. Information is a corporate resource and is to be managed as a corporate asset.

The organisation's overall information systems security policy must be responsive to legal and regulatory developments in many areas including the organisation's duty of confidentiality to its staff and customers, domestic and international data processing regulations, intellectual property rights and contract law.

The extensive and pervasive use of modern technology and changes in modern business practice require a specific formalised and central policy with respect to the security of information and the media and the environment in which data is input, stored, manipulated, displayed or transmitted.

By its very nature, security management implies control and restriction. However, these policies are not intended to constrain legitimate use, but to prevent unauthorised use of and access to information.

It is in the interests of all users and IT&T service providers that they read and follow the security guidelines set out in this document.

POLICIES

User identification

Userids and passwords uniquely identify individuals or groups of users of computer applications to ensure that access is appropriately authorised. The following policies define the principles applicable to the use of Userids and passwords.

- All password and Userids must comply with the VicRoads Password and Userid Standards.
- All passwords are to be kept confidential, and must not be displayed, shared or written down.
- Passwords are only to be reset in accordance with approved procedures.
- Any transaction of an auditable nature shall be traceable to an individual Userid.

Access to Computer and Data Resources

It is vital to ensure that access to computer and data resources is controlled to minimise the potential misuse of VicRoads business information and data, and to ensure the integrity of VicRoads computer systems.

- A User shall only have access to computer Application or Data resources on a business need basis.

- A User shall not try to access information for which they have no legitimate business need.

- A User's access to the Corporation's computer resources shall be:

    - cancelled immediately a User leaves the Corporation; or

    - reviewed and, if necessary, changed when a User changes duties, divisions or departments.

- Employees who have access to any form of information must not use, release, disclose, or study the information for any reason other than in the performance of their duties.

- No User shall use or attempt to use another user's logon.

- Access control shall be implemented on all IT&T platforms to ensure unauthorised access to the Corporation's computer resources is minimised.

- Access to data must be secured in accordance with the sensitivity of the data.

- All computer Applications and Data shall have designated owners who shall be responsible for all aspects of Application and Data management.

- The owner, or their designated representative, shall have sole responsibility to grant access to the computer Application or Data resources for which they are responsible.

Purchase and Use of Software/Hardware

- All Software and hardware purchased must comply with VicRoads purchasing guidelines and must be registered, as required, on the assets register.

- All purchased software is Corporation property.

- All vendor proprietary software must be used as specified in license agreements. Proof of purchase must be available for each serial number and each licensed software (and companion hardware) product.

- Only legally obtained software is to be used in VicRoads computing environment. The use of unlicensed or pirated software on VicRoads equipment is strictly prohibited.

- All traces of licensed software and data are to be removed from any hard disks remaining within equipment that is to be disposed of. Selective removal of data and software is to be done prior to equipment being internally transferred.

Virus Control

Computer viruses are a common risk to the security and integrity of business applications and data in the current computing environment. The purpose of this policy is to ensure that viruses are not introduced into the Corporation's computing environment, compromising the security and integrity of business applications and data.

- All electronic media brought into the VicRoads Information Technology (computer) environment shall be scanned for viruses using VicRoads approved and up to date virus scanning software. This shall be completed in accordance with the appropriate virus scanning procedures.

Backup and Recovery

- Appropriate backup and recovery procedures are to be in place for all corporate data and software. Interim manual procedures are to be developed and documented to manage vital business operations until computer facilities are restored. These procedures are to be tested on a regular basis.

Change Management

In order to minimise costly disruption to critical business systems, changes to computer applications and data must be controlled to minimise the possibility of data corruption, to ensure business systems can be recovered, and to ensure changes are appropriately documented.

- Modifications and maintenance to production applications will be subject to appropriate quality change control procedures.

- The Application Owner shall be responsible for ensuring that appropriate change control procedures are established and that system stakeholders are advised and consulted on proposed changes.

Data Ownership and Availability

VicRoads has significant investment in its data resources. In order to maximise this investment, data must be effectively managed by assignment of application owners who will be responsible for the quality and documentation of data under their control. The aim is to improve data consistency and accuracy, to readily accommodate new initiatives and changes in business requirements and allow effective data reuse.

- All data resources will have nominated business owners who will be responsible for the definition, accuracy, availability, accessibility and security of the data.

- All corporate data, unless specifically restricted for security reasons, will be appropriately documented and available for business purposes to VicRoads staff with appropriate access rights. Access to local data i.e. not corporate data) is to be arranged in consultation with the owner of that data.

- Data shall only be modified or destroyed in accordance with legislative and business requirements.

Disaster Recovery

The ongoing provision of critical computer systems is vital to business operations. Plans must be in place to ensure the timely and orderly recovery of software and data, continuation of business functions via interim manual procedures, and the effective update of data once systems are restored.

- Data and application owners shall ensure that vital business systems have adequately tested alternative processing procedures which are detailed in a documented Disaster Recovery Plan (DRP). The emergency procedures detailed in the DRP are to be included into the operating procedures of appropriate business areas. The plan is to be tested on a regular basis (recommended every 6 months).

Intellectual Property

- All information produced by or on behalf of the Corporation, regardless of format, is owned by the Corporation unless otherwise specified by a valid third party agreement.

- Design and development of information systems will be done using only properly acquired and authorised software and equipment. (i.e. Purchased, leased, licensed or public domain or software developed by VicRoads employees).

- Contracts with third parties, including contract staff, must define the ownership of the software.

- Software developed by or on behalf of the Corporation will remain the property of the Corporation and shall in no way be sold, copied, or in any other way used without the express permission of the Corporation or its authorised representative.

- Data, software and equipment are the property of the Corporation and use outside of the Corporation requires management approval. An employee noticing misuse or abuse of computer equipment, software or data must report it to their manager, their security administrator or the security co-ordinator in IT&T department.

Physical Access and Asset Protection

VicRoads computer assets and business information are vital resources that need to be protected from theft, loss or damage. VicRoads personnel must take all practical measures to ensure the protection of these assets and resources by allowing only authorised access to restricted areas, applications and data.

- Corporation computer hardware is to be physically protected from unauthorised access, theft. vandalism, destruction or environmental hazards.

- Only authorised personnel shall have access to restricted areas.

- During maintenance visits by non Corporation personnel all reasonable steps are to be taken to prevent the unauthorised access of information, or any activity which may subvert the system's operation or security.

- Measures shall be taken to reduce the risk of Corporation information being removed by maintenance personnel in failed components, diagnostic dumps, magnetic media or printed material.

Remote Access and Transmission of Information

The potential of 'hacking' into computer systems is a constant threat to the security and viability of information systems which have external network connections. It is vital that users are aware of the security risks and constraints of the technology they employ and follow appropriate guidelines and recommendations in its use.

- Transmission and access will only occur via authorised networks and using approved products.

- Remote access to the Corporation's computer systems must only be available to authorised officers.

- Modem phone numbers and/or any access procedural information must not be divulged to unauthorised persons.

- The carrier or service used for remote access or transmission of information shall ensure that the possibility of unauthorised communications or access to communicated information is minimised.

- Transmitting of data shall be done via a transmission medium that has the appropriate security measures commensurate with the sensitivity of the data being transmitted.

Using electronic information responsibly

- The VicRoads Network is a business resource and should be used in accordance with the Human Resources Code of Conduct and Ethics.

- Use of VicRoads corporate E-mail and Internet resources is approved for professional development activities and minor personal use that is without significant cost to VicRoads, excludes private business use, and is consistent with community standards expected of a government sector organisation.

- The VicRoads Network should be treated like any shared filing system and information may be subject to investigation.

- Employees sending or receiving messages are acting as officers of VicRoads and messages will remain the property of the Corporation.

- Electronic information is subject to the provisions of VicRoads policy to provide a work environment free from harassment as described in the Human Resources Manual.

- It is a violation of this policy for any employee to use the network for inappropriate distribution of material within the Network or through the Network to other electronic Public Networks, such as the Internet. Such action will be treated as misconduct and be subject to the Disciplinary Procedures set out in the Human Resources Manual.

- Line Managers are to report any incidents of misuse to the General Manager - Information Technology and Telecommunications in the first instance, who may be required to monitor the activity.

- Consideration should be given to encrypting sensitive or confidential legitimate business information that is to be sent via the Network.

- The content of information exchanged via the Electronic Network shall be appropriate and consistent with organisational policies and subject to the same restrictions as any other form of correspondence.

- Sensitive or confidential information must not be sent via the Internet unless encrypted.

- Do not share account numbers, passwords, user identification or other secure information.

- Messages and other material held on the network are documents in the possession of a Government Agency for the purposes of the Freedom Of Information Act and may, therefore, be the subject of a request under the Act.

- The VicRoads Network is not exempt from the copyright provisions which apply to the dissemination of information, recordings, images and programs in electronic form.

Penalties for Policy Non Compliance

Willful deviation from VicRoads Security policy and procedures will be treated as serious misconduct.

Any employee who knows of, or suspects, a breach of information security must report the facts immediately to his/her manager, the application security officer or the Manager IT&T.