Introduction

This procedure applies to:

- All users of Bega Valley Shire Council information, including service providers of Bega Valley Shire Council
- All information assets encompassing: facilities, data, software, paper documents and personnel.

The goal of information security is to protect Bega Valley Shire Council from adverse impact on its reputation and financial sustainability; litigation; impacts detrimental to the public interest; and disruption to services and operations, resulting from failures of:

- **Confidentiality**
  In the context of access or disclosure of the information without authority.
- **Integrity**
  In the context of completeness, accuracy and resistance to unauthorised modification or destruction; and
- **Availability**
  In the context of continuity and the business processes and for recoverability in the event of a disruption.

Council must comply with the *Australian Privacy Act 1988* Act no. 119 of 1988 as amended. Councillors, staff and contractors are also subject to the act.

Purpose

- Ensure the continuity of Bega Valley Shire Council and its services to its customers and business partners.
- Minimise the possibility of a threat to information security causing loss or damage to Bega Valley Shire Council, its customers and business partners.
- Minimise the extent of loss or damage from a security breach or exposure.
- Ensure that adequate resources are applied to implement an effective information security program.
- Identify the essential measures of the information security program.
- Inform all Bega Valley Shire Council personnel, other government agencies, customers and business partners who have access to Bega Valley Shire Council information of their responsibilities and obligations with respect to security.
- Ensure that the principles of information security are consistently and effectively applied during the planning and development of the Bega Valley Shire Council’s activities.
- Protect the privacy of individuals.
- Ensure that personnel are aware of information recorded for audit and tracking purposes in relation to their use of facilities, access to data, software and paper documents of council.
Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilities</td>
<td>Includes all equipment, as well as the physical and environmental infrastructure:</td>
</tr>
<tr>
<td></td>
<td>• Computer processors of all sizes, whether general or special purpose, including personal computers and mobile devices;</td>
</tr>
<tr>
<td></td>
<td>• Peripheral, workstation, printers, scanners and terminal equipment;</td>
</tr>
<tr>
<td></td>
<td>• Telecommunications and data communications cabling and equipment;</td>
</tr>
<tr>
<td></td>
<td>• Industrial and process control equipment;</td>
</tr>
<tr>
<td></td>
<td>• Local and wide area network equipment;</td>
</tr>
<tr>
<td></td>
<td>• Environmental control systems, including air-conditioning and other cooling equipment;</td>
</tr>
<tr>
<td></td>
<td>• Alarms, and safety equipment;</td>
</tr>
<tr>
<td></td>
<td>• Required utility services, including electricity, gas and water; and</td>
</tr>
<tr>
<td></td>
<td>• Buildings and building improvements accommodating personnel and equipment.</td>
</tr>
<tr>
<td>Data</td>
<td>Includes both raw and processed data:</td>
</tr>
<tr>
<td></td>
<td>• Electronic data files, regardless of their storage media and including hard copies and data otherwise in transit; and</td>
</tr>
<tr>
<td></td>
<td>• Information derived from processed data, regardless of the storage or presentation media.</td>
</tr>
<tr>
<td>Software</td>
<td>Includes locally developed programs and those acquired from external sources:</td>
</tr>
<tr>
<td></td>
<td>• Operating system software and associated utility and support programs;</td>
</tr>
<tr>
<td></td>
<td>• Application enabling software; including data base management, telecommunications and networking software</td>
</tr>
<tr>
<td></td>
<td>• Application software.</td>
</tr>
<tr>
<td>Paper documents</td>
<td>Include systems documentation, user manuals, continuity plans, contracts, guidelines and procedures.</td>
</tr>
<tr>
<td>Personnel</td>
<td>Includes employees, councillors, contractors, consultants, service providers, representatives of customers and other bodies that access the council’s information and data.</td>
</tr>
</tbody>
</table>

General principles


Applying risk management techniques, information assets shall be evaluated for the purpose of determining their individual value to Bega Valley Shire Council and for the selection of appropriate protection measures. The evaluation shall take into consideration the relevant legal and statutory compliance requirements.

Council must comply with the Australian Privacy Act 1988 Act no. 119 of 1988 as amended. Councillors, staff and contractors are also subject to the act and must therefore ensure information contained or stored on any device complies with the act and to ensure such information is neither lost nor exploited.
**Obligations**

The guiding principle is that controls in place shall be effective as measured against security standards and compliance requirements that are of particular relevance to Bega Valley Shire Council. These controls shall focus on the requirements outlined herein.

**Authenticity**

Users of information assets shall be uniquely identified to the information being accessed.

**Integrity**

There shall be adequate protective controls / safeguards to ensure completeness and accuracy during the capture, storage, processing and presentation of information.

**Confidentiality**

There shall be adequate protective controls / safeguards to ensure that information is disclosed only to authorised users.

**Availability**

There shall be adequate protective controls / safeguards to ensure that information can be delivered to Bega Valley Shire Council activities when required.

**Reliability**

There shall be adequate protective controls / safeguards to ensure that information available is complete and accurate.

**Accountability**

There shall be adequate protective controls / safeguards to ensure that responsibility for information undertaken by providers and users of information.

As part of undertaking adequate protective goals and safeguards, access to council’s facilities including areas that require use of a proximity or other access card, software, data and paper documents may be logged and audited, identifying personnel involved. This logged information may be used for internal auditing purposes as well as in any investigations into breach of council policy or code of conduct.

**Conduct**

Access to Information shall be solely for the conduct of Bega Valley Shire Council business; no private use, or use for any other purpose shall be permitted unless specifically approved by the General Manager, covered in policy 5.02 Behaviour of Councillors and Staff or described in an existing policy.

Usage of information must be able to survive public scrutiny and/or disclosure so as not to bring Council’s image into disrepute.

Usage of information must not be for any illegal purpose.

Information contained on or in equipment issued by ICT is considered and remains the subject of this policy and remains the property of the Council.

**Education and Training**

Bega Valley Shire Council recognise the importance of security education and the need for training and continuing education programs for all Bega Valley Shire Council personnel, customers and business partners.
Review

Compliance with the Policy will be monitored on a regular basis. Security logs and audit trails will be produced to monitor the activities of users in their usage of information assets. This policy, with its supporting guidelines and procedures, will be reviewed on at least an annual basis to ensure completeness, effectiveness and usability.

Responsibilities

The Managers responsible for Information Security (the Manager – Business Services for IT security and the Executive Manager – Organisational Development and Governance for hardcopy records), will coordinate the development of guidelines and procedures for the implementation of this policy, and will be responsible for an on-going review of their effectiveness. The Manager – Business Services must ensure that all personnel are fully informed of their obligations and responsibilities with respect to these guidelines and procedures.

All personnel, whether employees, Councillors, contractors, consultants or visitors, are required to comply with the information security guidelines, procedures and mechanisms and to play an active role in protecting the information assets of the organisation. They must not access or operate these assets without authority and must report security breaches or exposures coming to their attention to the relevant manager responsible for Information Security.

Managers have a responsibility as custodians of the data and other information assets that support the business activities performed under their supervision to ensure that those assets are adequately secured. They must also ensure that the appropriate information security guidelines, procedures and mechanisms are observed in the performance of these activities.

The Manager – Business Services and Senior Systems Engineer are responsible for the day-to-day administration of the information security procedures and practices. These staff report directly to the Managers responsible for Information Security on the performance of the information security procedures and practices.

Sanctions

Users who violate any of the conditions of this policy may be subject to disciplinary action including (but not limited to) written warnings and revocation of access privileges. Council is obliged to report any illegal violations to the appropriate authorities.

Other relevant documents

This procedure is to be read in conjunction with policy 5.09 Information Technology as well as policy 5.02 Behaviour of Councillors and Staff. It is also to be read in conjunction with procedures 5.09.1 Internet, intranet and email acceptable use and 5.09.3 Computer hardware & software acceptable use.
Attachment: Information Security agreement

I, (print name) ______________________________ acknowledge that I am being granted access to Council information in order to carry out my work and agree that my use of information will be conducted in an ethical and professional manner.

I agree that I will not use this access for personal use.

I understand that I have been given notice in accordance with section 10(2) of the Workplace Surveillance Act 2005 (NSW); and that Council will be entitled to, and shall commence monitoring, all my personal and business use of these services and communication facilities, and that monitoring will be in accordance with this policy and that **inappropriate usage may be cause for disciplinary action up to (but not limited to) written warnings and revocation of access privileges.**

I understand that my use of information is identifiable by others as a Council activity and acknowledge that it is my responsibility to ensure that my usage does not contravene any laws or regulations, including copyright and licensing.

I understand that I am to comply with the information security guidelines, procedures and mechanisms and to play an active role in protecting the information assets of the organisation. That I must not access or operate these assets without authority and must report security breaches or exposures to the relevant manager responsible for Information Security.

I understand that if I am not prepared to accept any of these conditions of this policy that access to social media will NOT be granted.

I understand that by signing this document that I acknowledge that I have read and understood this document. I further understand that it is my responsibility to seek advice regarding any questions that I might have regarding this document prior to my signing.

Signed ______________________________ Date ______________________________

Witness name ______________________________ Witness signature ______________________________