IM-Gov-7.1 Information Management and Communication Technology Policy

Policy

1. Primary Goals
    a. assure the use of information and technology generates business value to EV
    b. oversee management's performance and service delivery
    c. mitigate the risk associated with using information and technology.

2. Responsibilities
    a. The EV Board will oversee areas of ICT at a governance level and related policy
    b. The EV Senior Management team will oversee areas of ICT at an organisational level and related policy
    c. The IT Manager will oversee areas of ICT at an operational level and related policy.
    d. FARM will oversee the risk profile and appetite of IT

3. Strategy and Risk
    a. The IT strategy will align with the company strategic plan
    b. IT should endeavour to utilise and develop new and innovative solutions to improve service offering and quality to the company and its stakeholders
    c. IT should incorporate and maintain adequate safeguard measures, in line with acceptable risk and related statutory requirements.
    d. IT should meet contractual service levels and obligations as determined from time to time.

4. Supporting Policies
    EV has a suite of organisational and operational policies from which IT references and in some instances manages. The policies are presented during induction and readily available through the Document Library. The expectation is for IT Staff, related suppliers and users, to adhere and abide to the policies outlined below:

    a. IM-Org-7.1 Internet, Email and Social Media
    b. IM-Org-7.2 Computer System Backup and Security
    c. IM-Org-7.3 Media Liaison and Communication
    d. IM-Org-7.6 Management of Records

5. Controls and Monitoring
    IT utilises a variety of tools to monitor the activity and integrity of services. Results from monitoring and feedback are reported back to:
    a. Director of Corporate Services
    b. Senior Management Team

Definitions

Data breach – "The situation where personal information held by an agency organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference." (Office of the Australian Information Commissioner).

Malware – short for malicious software: – Computer programs/software designed to infiltrate and damage computers and systems. Can include viruses, worms, Trojans and spyware.

Information technology resources - include all information assets (e.g. databases, files and documents); software assets (e.g. applications and systems software and development tools); and physical assets (e.g. computers, communications equipment).

Social media: can be defined as the growing spectrum of online, internet-based tools and applications which people use to communicate. Examples of social media include but are not limited to:

- micro-blogging sites, e.g. Twitter
- social networking sites, examples include but are not limited to Facebook, , dating sites
- video and photo sharing sites, e.g. YouTube, Flickr
- weblogs, including corporate or personal blogs
- forums and discussion boards, e.g. Yahoo! Groups or Google Groups
- online encyclopaedias, e.g. Wikipedia
- social Bookmarking

Additional Information

- Office of the Australian Information Commissioner: Data Breach Guide 2014.

Relevant Legislation

- Health Records Act 2001
- Public Records Act 1973
- Freedom of Information Act 1982 (Commonwealth)
- Privacy Act 1988 (Commonwealth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Public Interest Disclosure Act 2013 (Commonwealth)

Title (including ID Number)		IM-Gov-7.1 Information Management and Communication Technology Policy			
Policy owner (position title)		CEO			
Date created		February 2016	**Date first approved**	April 2016	
Review history	**Date**	March 2017	October 2019		
	Version no.	02	03		
	Date				
	Version no.				
Date this version approved		February 2020	**Version no.**	03	
Approved by		Board			
Next review		February 2021			