Illawarra Shoalhaven Joint Organisation
Policy Manual

Cyber Security Policy

1. Policy Statement

Our Cyber Security Policy outlines:

- the technology and information assets that we need to protect
- threats to those assets
- rules and controls for protecting them and our business operations.
- the type of business information that can be shared and where
- acceptable use of devices and online materials
- handling and storage of sensitive material

Our Cyber Security Policy considers the following steps:

2. Procedures

1. Password requirements

All staff on joining our organisation will be issued with a system access password.

Under current arrangements a separate email password will also be generated.

In relation to these passwords:

- changes will only be made to passwords at the direction of the Executive Officer. In general circumstances, passwords will only be changed when a security breach has occurred (for example, a password has been accessed and used by a person who is not an ISJO employee)
- passwords must be kept secure and not be revealed to anyone outside our organisation
- passwords will periodically be updated
- under no circumstances should an ISJO password be used for a personal account (e.g. a Gmail account)

2. Email security measures

- Email communication is a basic business tool and the principal means by which we communicate with business partners, stakeholders and regulators. Staff email addresses will therefore be widely shared. The openness of our email should not blind us to the fact that individuals may seek to use our email addresses to inappropriately access and potentially damage our corporate systems and information.

  We should therefore:

  1. only open email attachments from trusted contacts and businesses
  2. be aware of and conform to any measures undertaken by our IT provider to block junk, spam and scam emails

3. identify, delete and report suspicious looking emails to the Executive Officer and / or our IT provider. Our email messages include notation of Message protection and a link to enable reporting of spam

> Message protected by Partner IT MailGuard: e-mail anti-virus, Anti-spam and Content filtering.
>
> Report this message as spam

4. All outgoing email correspondence should include a range of disclaimers and advice from ISJO in terms of email security and access.

   These messages will be automatically generated by the system and will be periodically updated. Advice on how these messages are to be inserted into emails will be provided to staff.

> This email message, together with any attachments, is for the exclusive and confidential use of the addressee(s). Any other distribution, use of, or reproduction without prior written consent of the sender is strictly prohibited. Should you have received this message in error please contact the sender immediately and then securely delete it. Views expressed in this email message are those of the individual except where specifically stated otherwise. Illawarra Shoalhaven Joint Organisation does not warrant or guarantee this message to be free of errors, interference or viruses

3. Handling sensitive data

Staff will from time to time have access to sensitive government and commercial data. When it comes to handling this sensitive data:

- staff may only share sensitive data with others within our organisation and with the State Agency or Council that may have provided it. In no circumstance is sensitive data to be shared with an individual or an organisation outside of ISJO, its member Councils or a State Government agency without the specific, prior and written permission of the Executive Officer
- storage of sensitive data in hard copy form or on portable storage devices should generally be avoided. If hard copy or portable copies of sensitive data are required they should be stored in a secure place. Almost without exception a secure place is within the ISJO Office
- hard copies of sensitive data should be destroyed when they are no longer required. ISJO will arrange secure disposal of these hard copies. Hard copies must never be placed in recycling bins.

Questions in regard to what constitutes sensitive data should be forwarded to the Executive Officer for advice.

4. Rules around handling technology

- Employees may be supplied with a laptop, iPad or similar electronic device to allow them to work away from the workplace. These electronic devices remain the property of ISJO and must be securely stored when they are not in use
- Electronic devices are to be returned to ISJO prior to the end of employment with our organisation
- Theft, loss of or damage to a work electronic device (including mobile phones) must be reported immediately to the Executive Officer

- System updates such as IT patches and spam filter updates will be installed and periodically updated. Staff given access to electronic devices must cooperate with any requirements required by our IT provider in regard to such measures
- Desktop and portable electronic devices must be shut down when not in use
- Screens should be locked when computers and devices are left unattended
- Generally speaking, data should not be stored on devices like USB sticks. If USB sticks must be used any data especially sensitive data should be securely wiped once access is no longer required. Advice on secure wiping may be obtained from our IT provider
- Software including games and other apps should not be installed on ISJO electronic devices. Prior permission of the Executive Officer is required for such installations to help protect against malware and other security risks
- All removable devices must be scanned for viruses before they are connected to our business systems. Advice on such scanning should be sourced from our IT provider.

5. Standards for social media and internet access

Our standards for social media and internet access include:

- A prohibition on the sharing of ISJO business information on social media channels without the prior written permission of the Executive Officer
- Staff being required to only use their work email account for ISJO related business. Private matters should be dealt with via personal email and / or social media accounts
- Websites and social media channels that are not related to ISJO business activities should generally not be accessed during work hours. Limited access during lunch breaks may be appropriate
- Inappropriate, illegal or otherwise unsuitable use of ISJO electronic internet or phone access is without exception prohibited. System use will be monitored and appropriate action undertaken via internet access alerts and other security measures
- ISJO staff may never use ISJO electronic equipment, email accounts or web pages to harass, vilify or threaten any individuals or groups. Staff may not use their ISJO positions or ISJO information or status on private social media channels without the prior written approval of the Executive

6. Prepare for an incident

If a cyber security incident occurs, staff should minimise the impact and get back to business as soon as possible. ISJO will therefore provide guidance on:

- how to respond to a cyber incident
- what actions to take
- staff roles and responsibilities for dealing with a cyber attack

Cyber security incident response plan

An incident response plan helps us prepare for and respond to a cyber incident. It outlines the steps we need to follow. Our Plan includes the following:

Prepare and prevent

- Preparing our business and employees to be ready to handle cyber incidents
- Developing policies and procedures to help us understand how to prevent an attack and to identify potential incidents
- Identifying the assets that are important to our business – financial, information and technology assets
- Considering the risks to these and the steps we need to take to reduce the effects of an incident
- Creating roles and responsibilities so we all know who to report to if an incident occurs, and what to do next.

Check and detect

We need to be able to check and identify any unusual activities that may damage our business information and systems.

Unusual activity may include:

- accounts and the network not being accessible
- passwords no longer working
- data being missing or altered
- hard drives running out of space
- computer persistently crashing
- our customers receiving spam from our business account
- staff receiving numerous pop-up ads

Identify and assess

- Finding the initial cause of the incident and assessing the impact so we can contain it quickly
- Determining the impact the incident has had on our business
- Determining its effects on our business and assets if not immediately contained

Respond

- Limiting further damage of the cyber incident by isolating the affected systems. If necessary, this will involve disconnecting from the network and turn off our computers to stop the threat from spreading

- Removing the threat
- Recovering from the incident by repairing and restoring our systems to business as usual.

Review

- Identifying if any systems and processes need improving and making those changes
- Evaluating the incident before and after for any lessons learnt
- Updating our cyber security incident response plan based on the lessons learnt so we can improve our business response.

7. Keeping our policy up-to-date

Our Cyber Security Policy will be reviewed and updated on a regular basis. Staff involvement in these processes will be important as will involvement and advice from our IT provider.