Data and Information Security Policy

This Policy applies to: All Employees, Volunteers and all Third Party providers

Policy Objective

This policy is to provide employees with clear guidelines regarding:

- ICLA's systems to maintain information and data security
- What constitutes a data breach; and
- What to do in the event of a data breach.

Policy

ICLA is committed to maintaining the privacy and security of data and personal information related to staff and the people we support. This commitment includes ensuring that in the event of a suspected or actual data breach, appropriate procedures are followed including notification to affected individuals and remedial action to prevent further breaches.

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. Personal information in this context is information about an identified individual, or an individual who is reasonably identifiable. The occurrence of a data breach in itself is not enough to make it eligible for reporting.

A notifiable or reportable data breach occurs when the following criteria are met:

1.

- Personal information is lost OR
- Personal information is disclosed to a third-party OR
- A third-party accesses personal information without permission

AND

2.

- The loss, access or disclosure is likely to result in serious harm to a person, AND
- ICLA as an organisation has not been able to prevent the likely risk of serious harm.

Details

ICLA has in place a range of measures designed to ensure confidentiality and privacy of data and information. These include:

- Policies and procedures governing privacy, confidentiality and data breach
- Monthly reporting to the Board on maintenance of privacy, confidentiality and data security
- Contractual arrangements with all third-party information technology and software providers include privacy compliance and support requirements such as monitoring, notification of breaches and regular upgrades to prevent unauthorised access.
- All ICLA staff, volunteers and Board members are required to provide a police check before working with the organisation.
- All ICLA staff, volunteers and Board members are required to sign the ICLA Code of Ethics and Conduct on commencement.

For the majority of the organisation's 30+ year history ICLA has operated on a paper-based system. ICLA has undertaken an organisation wide information technology (IT) systems project which involves transitioning from paper-based management of information and data to a secure, cloud based digital environment protected by multiple layers of security. This incorporates hardware and operating environment upgrades that include increased measures to maximise the cyber security resilience of the organisation such as single-sign-on and multifactor identification. The following controls are in place as of March 2019:

- ICLA data is stored on an iRAP certified Office365 environment via SharePoint and OneDrive.
- Email hosted on Office365.
- Multi Factor Authentication (MFA) is enabled.
- Password policies are in place to ensure they are complex and changed regularly.
- Critical company data is replicated to an alternate cloud provider.
- Endpoints are protected with Office365's enterprise mobility and security service with appropriate security controls in place administered through inTune.
- Endpoints are encrypted.
- Data at rest and in transit is fully encrypted (end-to-end)
- Endpoints are patched regularly through automation.
- All systems are monitored by Danet Technology using our Remote Monitoring and Maintenance Tools.
- Old paper files are archived securely with Iron Mountain, a records and document management facility. Records are kept for a minimum of 7 years.

Our IT provider (Danet) operates in an environment that has successfully passed iRAP certification. All Danet work is fully logged and Danet staff are required to pass police check in order to be employed. Danet assists ICLA with managing data and information, including destroying, storing and retrieving data.

As part of the systems upgrade, a new software system will form the basis of ICLA management of data and information related to the people we support. This system limits the information accessible to staff to be dependent on individual role and include alerts to manage client consents around sharing of information. For example, front line support staff

have access only to critical information required for daily support on the day of service. Access to the full system is limited to our Management level staff.

Our system includes:

Enrite Care

Enrite Care is a Client Data Information Management System (CDIMS) which operates on the Salesforce platform. Salesforce has received security certification by the Australian Signals Directorate (ASD), which governs and regulates information privacy and security for Australia's government agencies.

Salesforce received the accreditation through the Information Security Registered Assessors Program (IRAP) as part of the ASD's Certified Cloud Services List (CCSL) for 'Unclassified DLM' data, across the core Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) cloud offerings. This accreditation gives Salesforce customers in Australia the additional assurance that its privacy and security program meet the high standards recognised by the ASD.

Easy Employer

ICLA currently uses Easy Employer to maintain employee records. Kronos will replace Easy Employer as ICLA's human resource management software in 2020.

Kronos

ICLA will implement Kronos in 2020 as a human resource management software. Kronos will contain data for all ICLA's employees, with plans to extend to a Time in Attendance system to manage rostering and timesheets.

Confidential information

Employees are responsible for taking measures to prevent the use or disclosure of confidential information. This includes following ICLA's policies and procedures regarding personal and confidential information and using ICLA's established information management systems.

Employees are expected to use their own mobile phones for work purposes under ICLA's Bring Your Own Device (BYOD) policy. All employees are required to install the Microsoft Authenticator application on their device, which requires a second layer of authentication to access ICLA systems. This requirement is in place to protect the security of any ICLA information that could be accessible on an employee's device.

Employees are only to access ICLA systems in the course of their work-related duties. Employees who no longer require access to ICLA systems for work purposes will have their

access to systems blocked to ensure the security of data. If an employee is suspended their access will be blocked for the duration of their suspension.

The following applies to all employees of ICLA, both during and after their employment with ICLA.

Employees will:

- Not directly or indirectly disclose, copy or use any confidential information for their own benefit or the benefit of any other person or entity, except in the proper performance of their duties or within the written consent of ICLA;
- Keep any confidential information secret and confidential, except to the extent they are required by law to disclose it; and
- Take all reasonable and necessary precautions to maintain the secrecy and prevent the disclosure of any confidential information.
- Immediately notify ICLA if they are lawfully obliged to disclose any confidential information to a third party, and must comply with ICLA's lawful directions in relation to the disclosure.

On termination of employment, or at any time if requested by ICLA, employees must return all confidential information, and provide ICLA with copies, extracts and notes or recordings of the confidential information.

Surveillance

ICLA may conduct surveillance of Information Technology systems, in line with the Workplace Surveillance Act 2005, to ensure the security of personal and confidential information and data. This may include computer surveillance, being surveillance of all ICLA's IT hardware and software computer systems and their use (including email and internet use).

The new Kronos system will require employees to enable location settings on their mobile phones. ICLA will use geofencing to prohibit people from logging into their shift if they aren't within a specified radius of the location of their shift.

DEFINITIONS

Data breach	Occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. The occurrence of a data breach in itself is not enough to make it eligible for reporting – it must meet the criteria outlined above.
Confidential information	All information (whether or not it is described as confidential) in any form or medium concerning any past, present or future

	business operations or affairs of the employer, clients (people we support), contractors or suppliers of the employer.
Personal information	Information about an identified individual, or an individual who is reasonably identifiable.

Legislation and/or Reference Documents

Privacy Act 1988 (Commonwealth)

Workplace Surveillance Act 2005 (NSW)

Associated Documents

ICLA Code of Ethics and Conduct

Data Breach Response Procedure

Thank you

We're here to help.

Get in contact for more information.

T +61 2 9281 3338
E hr@icla.org.au
W icla.org.au

Independent Community Living Australia
Everyday life changing