BLAND SHIRE COUNCIL
west wyalong

# PROCEDURE

# INFORMATION SECURITY INCIDENT MANAGEMENT

**PROCEDURE ADOPTED: 18 August 2020**

---

**Procedure Objective:**
To ensure all staff and Council's IT contractors are properly informed of any information security incident.

**Policy Statement:**
This procedure aims to support all staff, contractors, third parties and service providers the appropriate information to report an information security incident.

**Definitions:**
***Council*** – being Bland Shire Council

***Information*** – includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, communicated using social media.

***High Risk Confidential Information*** – This can be summarised as:

- Any personal information that would cause damage or distress to individuals if disclosed without their consent
- Any other information that would prejudice Council's interests if it were disclosed without authorisation.

***Medium Risk Confidential Information*** – This can be summarised as:

- Any personal information that the individuals have not agreed to share e.g. lists of staff who have not completed training
- Any other information to which access must be limited on a business need to see basis e.g. a draft report

***Information Security Management System*** – That part of the overall management system based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

**Responsibilities:**
All users who are given access to Council information, IT and communications facilities have a responsibility to:

- Minimise the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it
- Protect the security and integrity of IT systems on which vital or confidential information is held and processed
- Report suspected information security incidents promptly so that appropriate action can be taken to minimise harm

**Recommended Practices:**
**Incident Identification**
Each individual may have a different interpretation of what a security incident is. The following list provides a few basic examples of what should be reported as an incident but is by no means an exhaustive list.

- A compromised account (Eg. Email account)
- Lost or stolen IT equipment (Eg. Laptop, phone or USB)
- Unusual network activity
- Attempted unauthorised access

***The golden rule is "If in doubt…..report".***

**Incident Reporting**
If an incident has been identified or suspected:

- Immediately
    1. unplug the network cable from your computer and from your servers,
    2. call your IT support person
        - Rhiannon Young - 279
        - Veritech 02 6964 5377

***It is imperative that a timely response is undertaken in security incidents; please notify either of the above ASAP.***

If you have any questions relating to this procedure email: IRequests@blandshire.nsw.gov.au

**Appendices:**
NIL

**Authorisation:**

| | | | |
|---|---|---|---|
| **Status** | **Committee** | N/A | |
| | **Manex** | 3 July 2018 | |
| **Owner** | **Director Corporate and Community Services** | | |
| **EDRMS Doc. ID** | 618910 | | |
| **Superceded Policy** | | | |
| **Date of Adoption/ Amendment** | **Revision Number** | **Minute Number** | **Review Date** |
| 3 July 2018 | | | July 2023 |
| 18 August 2020 | | | July 2023 |

| **Related Council Policy / Procedure** |
|---|
| Code of Conduct |
| Records Management Procedure |
| Access to information Policy |
| Internet Email and Computer Usage Policy |
| Privacy Management Plan |
| Information Security Incident Management Policy |