2.6   Information Technology – Incident Management Policy

POLICY STATEMENT
The Shire of Cunderdin has an obligation to ensure quick detection of, and response to, security events and incidents within the Information and Communications Technology (ICT) systems belonging to the Shire.

APPLICATION
Each employee, supplier, and other third-party, who is in contact with information or systems of The Shire, must report any system weakness, incident, or event which could lead to a possible incident. These incidents should be reported in the following way:
   a. All information and communication technology-related events must be reported to the Information Technology Service Area.
   b. Incidents, weaknesses, and events must be reported as soon as possible, by phone or in person.
   c. Incidents and events are reviewed and classified as part of the ICT Security and Operations Meeting. Incidents are classified as either:
   d. **Minor Incident** – an incident that is unlikely to significantly impact the confidentiality or integrity of information and is unlikely to cause long-term unavailability.
   e. **Major Incident** – an incident that may be likely to incur significant damage due to loss of confidentiality or integrity of information or may cause an interruption in the availability of information and/or processes for an unacceptable period.

Incidents will be recorded in the Incident Management Register where each event will be categorised according to their severity. Measures to contain the incident will be taken as per procedures outlined in the Incident Management Register.

OBJECTIVE
To accurately document any ICT security breaches. To better plan and respond to any incidents that may result in the Shire incurring, due to loss of confidentiality or integrity of information or may cause an interruption in the availability of information and/or processes of the Shire for an unacceptable time period.

If effective information security incident management is not accomplished, the likelihood and severity of incidents are increased greatly. Where possible mitigation strategies will be documented and reviewed in the Incident Management Register and where appropriate the risk register will be updated.

STATUTORY CONTEXT
Local Government Act 1995
Local Government (Audit) Regulations 1996

CORPORATE CONTEXT
Policy Manual
Strategic Community Plan
Incident Management Register
Internet, Email and Computer Use Policy

HISTORY
Adopted   23rd July 2023
Revised   _____

REFERENCES