POLICY:-	
Policy Title:	Electronic Security Systems Policy
File Reference:	F10/618-09
Date Policy was adopted by Council initially:	18 February 2010
Resolution Number:	76/10
Other Review Dates:	21 March 2013
Resolution Number:	65/13
Current Policy adopted by Council:	15 August 2019
Resolution Number:	212/19
Next Policy Review Date:	2022

PROCEDURES/GUIDELINES:-	
Date procedure/guideline was developed:	N/A
Procedure/guideline reference number:	N/A

RESPONSIBILITY:-	
Draft Policy developed by:	Director of Finance and Administration
Committee/s (if any) consulted in the development of this Policy:	N/A
Responsibility for implementation:	Director of Finance and Administration
Responsibility for review of Policy:	Director of Finance and Administration

Objective

The purpose of this policy is to provide a framework for the authorisation and control of the electronic security system for the Upper Lachlan Shire Council's Crookwell Administration Office buildings.

The Electronic Security Systems (ESS) is used to increase the general buildings security and limit the access to the Council Administration buildings. The ESS provides a high level of security for the designated buildings and is used as a tool to control, monitor and restrict the flow of persons to certain areas or buildings. This increases compliance with the work, health and safety requirements by providing staff with improved personal safety as well as enhancing the security of cash and equipment.

Scope

This policy applies to the Upper Lachlan Shire Council Administration Office building sites located at 44 Spring Street, Crookwell.

The security measures adopted include, but are not limited, to the following:-

- The security access control system is by security fob issued to individual Council employees and Councillors;
- The security access level and time period specific access is set for individuals, based on the respective position that employee holds with Council; and
- The Council's ESS allows the logging of all security access activity into the designated office buildings.

Responsibilities

<u>Systems Administration and Monitoring Responsibilities</u>

The approval and issuance of all ESS individual security access fobs to Council authorised personnel is the responsibility of the Information Systems Support Officer.

In the absence of the Information Systems Support Officer, the responsibility for the day-to-day building security access requirements will be the Manager of Finance and Administration.

The Information Systems Support Officer will be the electronic security system administrator for the Council buildings and is responsible for:-

- Remotely monitoring the system functions;
- Operate, administer and maintain perimeter entrance access controls for designated buildings;
- Issuing security fobs to individual Council personnel in conjunction with user requirements;
- Validating a security fob for use;
- Maintaining a register or database of all security fob holders;
- Identification and matching of security fob with the person who was issued a fob;

- Cancelling or deactivation of any security fob reported as missing or lost immediately upon such notice;
- Deleting access of a security fob held by departing personnel when managing the register;
- All unused security fobs will be deactivated and securely stored at the Crookwell Office;
- Retrieving any security fob from the relevant Departmental Manager received from departing personnel; and
- All maintenance responses and liaison with the ESS contractor to correct access faults, register database errors, door lock errors, public holidays and emergency access related issues.

Buildings Security Access

The relevant Council Departmental Director controlling a building is responsible for providing the Information Systems Support Officer with all relevant details relating to security access for each individual employee. This includes:-

- Determining the areas of access within the building;
- Determining the times of access to the building;
- Supplying the Information Systems Support Officer with a detailed access list; and
- Conducting regular audits of security fob issues and returns.

Security Access Levels

The door access level allocated to individual Council personnel; i.e. providing the conditions under which that security fob can be used are created by the Information Systems Support Officer after authorisation from the relevant Departmental Director and / or Manager concerned. The level of access permitted to individual staff members will be as determined by senior management.

Conditions of Usage

The individual employee and individual Councillor are responsible for the safe storage of the security fob issued to them and are accountable for that fob at all times.

Security fobs are issued to the individual for their personal use only and are not to be lent or transferred to anyone else. Any staff member found to have allowed unauthorised use of their security fob will be subject to disciplinary action.

An individual is to immediately report to their Departmental Director if there is a security fob which is lost, missing or has been found. The Departmental Director is to immediately liaise with the Information Systems Support Officer to arrange deactivation or cancelling of a security fob.

If an individual employee wishes to amend their security fob access rights and conditions they must report to their Departmental Director. The access rights will be amended only after signed approval from the relevant Departmental Director.

Council Departmental Directors, Managers and Supervisors are responsible to ensure the continued understanding of the policy and its protocols by Council staff.

Abuse or Misuse of Security Access

Any user who, in the opinion of the Council's General Manager or by their delegated authority is considered to have abused or misused the security access fob to gain unlawful or improper access to Council facilities, assets and information will have their security access removed and disciplinary procedures shall be instigated. If the incident is deemed serious enough the matter will be referred to the NSW Police for investigation and / or the Independent Commission Against Corruption (ICAC) if necessary.

Relevant Legislative Provisions and Council Policies

Reference should be made to the following legislation, guidelines and policy documents when reading this policy:-

- Industrial Relations / Workplace Surveillance Act 2005;
- Local Government Act 1993;
- Local Government (General) Regulation 2005;
- Work Health and Safety Act 2011;
- Local Government (State) Award 2017;
- Privacy and Personal Information Protection Act 1998;
- Government Information (Public Access) Act 2009;
- State Records Act 1998;
- Fair Work Act 2009;
- Independent Commission against Corruption Act 1988;
- Anti Discrimination Act 1977;
- Council's Code of Conduct;
- Council's Complaints Management Policy;
- Council's Internet and Email Policy;
- Council's Disciplinary Policy;
- Council's Fraud and Corruption Prevention Policy.

Review of Policy

Council reserves the right to review, vary or revoke this policy.