3.01 – ACCESS TO FINANCIAL MANAGEMENT SYSTEMS POLICY

1. INTRODUCTION

The purpose of this policy is to define the security requirements for staff and external parties who have access the Norfolk Island Regional Council's (NIRC) Financial Management Systems (FMS). *The Privacy Act 1988 (Cwlth)* and the 13 principles contained within the Act extend to Government Agencies on Norfolk Island, including the NIRC.

2. POLICY OBJECTIVE

The policy aims to ensure that effective control measures are in place to manage persons who have access to Councils financial information systems.

Adequate regulation and supervision enables Council to protect the privacy of individuals and organisations and meet its obligations under The Privacy Act 1988 (Cwlth) as well as reduce the risk of fraudulent activity.

3. POLICY SCOPE

This policy covers access by:

- *All employees of NIRC, including casual, contracted and volunteer staff*
- *Councillors*
- *Norfolk Island Police employees*
- *Consultants, auditors or other specialists*
- *Contract IT support personnel*
- *Designated Commonwealth staff*

To the following financial (FMS) systems under licence to the NIRC:

- *Smartstream*
- *ERP*
- *Attache*
- *RSAPOS*
- *Telstream*
- *Civica – Authority*
- *Civica – BIS*

4. DEFINITIONS

NIRC – Norfolk Island Regional Council
GM – General Manager
FMS – Financial Management Systems
ERP – Enterprise Resource Planning
RSAPOS – Retails Systems Australia Point of Sale
IT – Information Technology

5. LEGAL AND POLICY FRAMEWORK

The Privacy Act 1988 (Cwlth) extends to Government Agencies on Norfolk Island including the Norfolk Island Regional Council (NIRC). Schedule 1 – Australian Privacy Principles sets out the obligations of organisations when collecting, storing, providing access to and using private information.

See also, Local Government Act 1993 (NSW)(NI), Section 739 Protection of privacy.

6. IMPLEMENTATION

6.1 Roles and Responsibilities

The following Council officers are responsible for the implementation of and the adherence to this procedure:

Customer Care Manager
IT Officers

6.2 Support and Advice

The following Council officers can provide support and advice on this procedure:

Customer Care Manager
IT Officers

6.3 Communication

The procedure will be communicated utilising the Norfolk Island Regional Council's Intranet page and emailed to Executive Management and Managers to forward to their teams.

6.4 Associated Documents

New User FMS Access Request

7. POLICY

7.1 Access

Access to Councils FMS is restricted to authorised officers only.

Personal access information such as user name and password are not to be shared with any other person/(s).

Accessing Councils FMS systems using another authorised persons login is prohibited.

7.2 Responsibility

It is the responsibility of the Team Leader / Manager and/or Group Manager to authorise access to Councils FMS and to manage the use of these systems, as well as to ensure that staff members and contractors are aware of their responsibilities under this policy.

If an employee believes that their access to a FMS system has been compromised, or that their login information has been made known to another user then it is the responsibility of the employee to notify the IT Department and to change their password immediately.

7.3 Requesting Access to FMS Systems

All requests to access Councils FMS, including modifications to existing permissions, must be made in writing to the IT Department with the authority of the Group Manager. Verbal requests by staff will not be actioned.

7.1.1 Request Access for a New Employee

Complete the form *New User FMS Access Request* scan and/or deliver to the IT Department.

7.1.2 Modify access for an existing FMS user

The Group Manager is to email the IT Department spiceworks@nirc.gov.nf with written authority.

7.4 Suspension of Access to FMS

IT Officers have the authority to suspend temporarily an employee's access to FMS if they believe that access has been compromised or used in any way for unauthorised use. If an employee's account is suspended the IT Officer who actioned the request will notify the Manager and/or Group Manager and clarify the reasons that the suspension was applied. Access will be reinstated after written approval is received from the Group Manager.

If an employee is suspended from work as part of a disciplinary process the IT Department must be notified immediately to enable suspension of access to FMS and other applications.

7.5 Termination of Access to FMS

A Manager may request that an employee's access to FMS be revoked at any time. Requests must be made in writing to the IT Department with the authorisation of the Group Manager.

In the instance where a staff member has their employment with Council terminated the IT Department is to be notified immediately to enable the removal of access to FMS and other applications.

When a staff member resigns from Council it is the responsibility of the employee's Manager to inform the IT Department of the date in which access to FMS and other applications is to be removed.

8. REVIEW AND VERSION CONTROL

Policy Number	3.01		Responsible Officer	Customer Care Manager
Effective Date	15 March 2017		Next Review Date	2020
Version Number	**Version**	**Resolution No.**	**Effective Date**	**Version description**
	V1	2017/36	15 March 2017	Developed and adopted