Corporate Information CMP

Corporate Information Compliance Monitoring Program (CMP)

Introduction

Council's vision for information management is "To provide easy access to reliable information anywhere and anytime through compliant and integrated systems". To help achieve this vision, a key component of Council's Information Management Strategy is to conduct regular audits of Council's information management program and monitor staff adherence with policy and procedures to ensure legislative compliance and continuously improve.

An assessment against Public Record Office Victoria (PROV) Recordkeeping Standards performed in XXX indicated that there was a lack of formal auditing of Council processes and systems in relation to information management. Non-compliance with mandatory standards issued by PROV under the *Public Records Act 1973*, can result in complaints, penalties, reputational damage and lost litigation.

Purpose

The purpose of this program is to conduct regular compliance audits to monitor the extent to which the Council is operating in accordance with its information management policy and procedures. This document has been developed to support requirements of the PROV Recordkeeping Standard for Strategic Management (PROS 10/10).

The program is operated by the Corporate Information Team. The program owner is the Manager XXX.

Scope

The program applies to all Council departments and compliance with the following areas:

- Information Management Strategy & Policy
- PROV Recordkeeping Standards
- *Public Records Act 1973*
- *Freedom of Information Act 1983*
- *Privacy and Data Protection Act 2014*
- EDRMS (XXX) Usage
- EDRMS (XXX) Business Rules

Objectives

The objectives of this program are:

- Regularly measure the level of compliance with Council policy and legislative requirements
- Identify and mitigate information management risks across Council
- Continuously identify opportunities for improvement for information management

Monitoring Program

The program will operate on an annual audit cycle; it is comprised of four audit activities and biannual compliance reporting, as shown below.

Table 1: Annual Audit Cycle

Activity	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
IM Framework Review								●				
Departmental Audits	●	●	●	●	●	●	●	●	●	●	●	●
Storage Inspections	●						●					
System Monitoring		●		●		●		●		●		●
Compliance Reporting			●						●			
Actions Reporting	●	●	●	●	●	●	●	●	●	●	●	●

Information Management Framework Reviews – Annually

Every August, Council's Information Management Framework will be reviewed by the Coordinator Corporate Information to ensure it is being maintained in accordance with the PROV Recordkeeping Standards.

The review will include the following:

- Confirm that annual reviews have been conducted on the following key documents:
    - Information Management Strategy
    - Information Management Policy
    - Corporate Information Customer Service Charter
- Verify that Information Management Procedures and Records Manager Business Rules are up-to-date
- Verify that all current outsource contracts include PROV compliant recordkeeping clauses
- Review any Privacy and FOI complaints received in the last 12 months to identify any recurring issues

The results of this review will be reported to the Manager XXX.

Departmental Audits –Monthly

Every month, one Council department will be audited by the Corporate Information Team to measure the extent to which they complying with areas in the records and information management program. This will allow each department to be audited once a year.

The audits will include the following:

- Assess the capture rate of significant emails into the EDRMS with selected staff by reviewing a sample of significant emails sent and received during the previous month
- Check EDRMS metadata quality on a sample of records registered by staff in the previous month
- Audit key or high-risk business processes to determine if full and accurate records have been kept for a sample of transactions
- Inspect locally stored paper files to determine if they have been registered in the EDRMS or contain unregistered records
- Inspect the contents of secure destruction bins to determine if records have been disposed of without authorisation
- Verify that Privacy Disclaimers have been completed when the collection or use of personal information has changed in the Department in the last 12 months

The results of these audits will be reported to Department Coordinators and Managers.

Storage Inspections – Biannually

Every January and July, all storage areas for inactive records (excluding offsite storage at the Approved Public Record Office Storage Supplier) will be inspected for compliance with the PROV Storage Standard by the Corporate Information Officers. A register of storage areas will be maintained and reviewed prior to the inspections, to determine if additional areas are in uses which need to be added and inspected.

Each storage area will be physically inspected for the following:

- Compliance with relevant requirements in the PROV Agency Records Storage Specification (PROS 11/01 S1)
- Workplace safety issues (e.g. trip hazards)
- General maintenance and cleanliness (e.g. leaking pipes, dust)
- Integrity of a sample of records in storage (e.g. pest infestations, mould, corrupt data files)

The results of these inspections will be reported to the Coordinator Corporate Information.

System Monitoring – Bimonthly

Every second month, a series of system monitoring reports will be generated and analysed by the Corporate Information Team to identify systematic non-compliances with the Information Management Policy.

Reports to be generated and reviewed include the following:

- XXX usage rates to identify staff that are not utilising the EDRMS
- Sensitive record security checks to identify records that have not been appropriately secured
- Home folder usage to identify staff that are not routinely moving finalised records to corporate files
- Network drive and desktop usage to identify folders that are being used to store new records

- USB device usage to identify staff that may be storing records outside authorised systems

Reports will be distributed to Department Co-ordinators for follow-up.

Actions Reporting

Every month, a series of actions reports will be generated and distributed by the Corporate Information Team to identify actions in progress, completed or overdue within the EDRMS.

Reports to be generated include the following:

- Councillor Correspondence Reports
    - First week of each month – All open requests addressed to a Councillor
    - First week of each month – All open request received from a Councillor
    - Second week of each month – All open requests received from a Councillor
    - Second week of each month – All completed requests received from a Councillor in previous month
- Monthly Overdue Actions Reports for all Council Divisions and Departments

The Councillor Correspondence Reports are provided to the Councillor Support Team and they then distribute to the Executive Team and Councillors. The Overdue Actions reports will be distributed to Executive Team, Department Coordinators and Managers.

Monitoring Process

The compliance monitoring process will operate continuously during the audit cycle. The key stages in the monitoring process are outlined below. Details on how to perform these processes are documented in the Information Management Compliance Monitoring Procedure.

Stage 1: Data Collection & Analysis

Data will be collected and analysed by the Corporate Information Team to identify compliance gaps, trends and risks through the audit activities detailed in procedure. System reports required for this program will be developed and maintained by the Information Technology unit. All audit data will be routinely recorded in the EDRMS.

Stage 2: Reporting

System, audit and inspection reports detailing the results and required actions will be prepared as part of each audit activity and distributed to relevant stakeholders for their information and action. Stakeholders will be provided the opportunity to review draft reports to correct any factual inaccuracies and comment on the feasibility of any proposed actions. A summary of all compliance monitoring results and audit actions (completed, pending and overdue) will be reported to the Manager XXX every six months. Any significant risks identified are to be added to the Corporate Risk Register.

Stage 3: Action Monitoring

All audit actions will be recorded in a central, electronic register stored in the EDRMS. Actions will be assigned an owner, priority and due date for completion. The Coordinator Corporate Information will mark actions as complete in the register when

advised by the action owner and Coordinator Corporate Information is satisfied the actions have been appropriately implemented. The status of all outstanding audit actions will be reviewed with the action owner when preparing the biannual compliance reports.

Stage 4: Overdue Action Escalation

Any overdue audit actions listed in the biannual compliance reports will be escalated to the Manager XXX for action. Overdue actions that are still overdue by the next biannual compliance report will be reviewed or cancelled by the Manager XXX.

Roles and Responsibilities

EDRMS Administrator

- Schedule and coordinate departmental audits
- Prepare departmental audit reports and distribute to relevant department heads and General Managers
- Analyse and distribute system reports to change agents
- Conduct departmental audit activities on a monthly basis
- Generate system reports on a monthly basis
- Generate action reports on a monthly basis

Corporate Information Officers

- Conduct biannual record storage area inspections
- Prepare record storage area compliance reports

Coordinator Corporate Information

- Coordinate the implementation of any remedial actions for record storage areas
- Conduct annual information management framework reviews
- Conduct monthly CI customer service charter audits.
- Prepare biannual compliance reports for the executive
- Monitor the completion of all audit actions
- Review the compliance monitoring program annually
- Ensure identified significant risks are entered into the Corporate Risk Register

IT Team

- Reports for System Monitoring (Network Drives, USB's, Home Drives)

Manager **XXX**

- Review and distribute compliance reports to the executive team
- Escalate overdue audit actions as required.

Program Review

The Coordinator Corporate Information will review the effectiveness of this program on an annual basis following the completion of the September compliance report. Amendments to this program must be authorised by the Manager XXX.