Government of **Western Australia**
Department of **Corrective Services**

Policy Directive 35

Custodial Business Processes (TOMS)

Context

All information that needs to be recorded, relating to offenders is to be retained in confidential electronic, paper or other media files. The effective management of these files underpins the organisation's capacity to operate effectively. As the responsibility for maintaining these files rests with a variety of officers it is essential that each officer observes a common set of protocols and procedures to ensure the highest standards are maintained with regard to record keeping.

Purpose

To ensure that all custodial records comply with principles outlined in this Policy Directive.

Definitions

Offender: For the purposes of this Policy Directive any reference to an offender in this document shall be interpreted to mean adults or juveniles held in prison.

1. Principles

- All information that is recorded on any official file is a confidential, legal record.
- All information that is recorded forms part of an official audit trail.
- Access to information is restricted to information required for official duties.
- Except where expressly approved otherwise, all recording officers must always clearly record the subject matter, their name, title, and date of finalising the information.
- Where information is retained on other officially sanctioned media (visual, audio, digital, etc) official standards and procedures relevant to each particular media shall be adhered to.

2. Strategies

2.1 A common, integrated set of records is to be maintained and used by all officers (including contractors) to record information as required.

2.2 Custodial business process records are the property of the Department of Corrective Services and are to be retained, released and disposed of in accordance with legislative and Department of Corrective Services requirements. Please refer to Records Management Procedures as set out by the Administrative Records Management Section of Information Services.

2.3 Offender-in-Custody files are held by the Offender Records Branch, Corporate Support, Knowledge Management. Offender-in-Custody files are to be normally kept for 5 years following release by Department of Corrective Services, and are generally archived for a further 70 years.

2.4 On receipt of an offender, officers are to ensure that existing and/or historical records are obtained, created and distributed (as required) expeditiously.

2.5 Unit Managers are responsible for ensuring that a Unit File is created for each prisoner, which contains all necessary documents. Documents may be removed, where appropriate, for imaging, and/or for inclusion in the Offender-in-Custody file.

2.6 Unit Managers are responsible for ensuring that when an offender is transferred, their Unit File is also transferred at the same time.

2.7 It is essential that Superintendents issue procedures governing the transfer of Unit Files to ensure they are delivered intact and in a manner that preserves the confidential nature of its content.

2.8 When an offender is discharged, all original records are to be transferred to the offenders central file.

3. General Instructions

- The business processes outlined above in Appendix 1 are to be maintained in an efficient and timely manner.
- The user processes referred to in Appendix 1 are to be utilised in conjunction with the TOMS (and other systems) user guides, training guides, on-screen help information, hint sheets, Jstaff and CSinet-based help information, Toms Access Policy, Director General's Rules, policy directives and any other relevant orders.
- Superintendent's and other prison service providers are responsible for ensuring that their business processes are compatible with these processes.
- Superintendent's and other prison service providers are responsible for ensuring that TOMS updates are communicated and adhered to by TOMS site representatives, workplace trainers and end users.
- The issuing of staff roles that control access to information is to be managed in accordance with the TOMS Access Policy.
- Officers are responsible for all data changes they make and must be signed on to the TOMS system using their own password.
- Generic passwords (Windows NT only) may only be used where specifically authorised by the Assistant Commissioner Custodial Operations.
- Staff may only access information required to perform their official duties as at the time of access. Browsing of records and/or accessing records of offenders at other facilities may be deemed as unauthorised access.
- Officers may impart data to another staff member, while signed on under their own password, provided no changes are made to the TOMS database and providing the information is required as part of the requesting staff members official duties.

4. General

Superintendents and prison service providers are to prepare and issue instructions and procedures that ensure compliance with the DCS custodial business process requirements, including TOMS process requirements, as set out in Appendix 1.

Applicability

This applies to all prisons.

This Policy Directive does not apply in relation to medical records. See instead Policy Directive 17.

Policy Sponsor

Assistant Commissioner Custodial Operations

Contact Person

Principal Operational Policy Officer