Data Control Policies for the District Six Medical Examiner and Pinellas County Forensic Laboratory

Policy Statement

For purposes of establishing guidelines in conformity with the requirements of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), specifically, ISO:IEC 17025:2005 General Requirements for the *Competence of Testing and Calibration Laboratories, Section 5.4.7 Control of Dat*a and the ANAB/LAB Supplemental Documents. ISO 17025 is the international standard for quality systems in testing and calibration laboratories used as the basis for accreditation of forensic testing laboratories.

Pinellas County maintains an annual agreement for the services of the District Six Medical Examiner that includes the Pinellas County Forensic Laboratory. The agreement includes providing technology support that is managed by Pinellas County Business & Technology Services (BTS).

1. Scope

a. For purposes of the policy the scope is defined as all software, data and systems maintained by BTS on behalf of the Medical Examiner's office.
b. A complete list of in scope items will be maintained in Appendix A of this policy.
c. Appendix A is to be reviewed, updated and agreed by both parties on an annual basis.

2. On and Off Boarding of Medical Examiner and Forensic Lab Employees

a. For application and systems that BTS facilitates access control, all access will be granted with approval from the Director of the Forensic Laboratory or Director of Investigations consistent with employment policies and job description.
b. For application and systems that BTS facilitates access control, access will be removed from upon notification from the Director of the Forensic Laboratory or Director of Investigations as consistent with employment policies.
c. For audit purposes, documentation of access approval and/or access revocation must be maintained for 5 years.
d. BTS will provide annually or on an as needed basis a list of accounts (both BTS and Medical Examiner), systems and levels of access for all systems listed in Appendix A where BTS is responsible for access control.
e. All remote access to Medical Examiner systems and data requires a Remote Access (VPN) form to be filled out and signed by the Director of the Forensic Laboratory or Director of Investigations.
f. On and Off Boarding will be conducted per the BTS on and off boarding procedure.

3. Protection of Data

a. BTS protects all data and systems based on the needs and requirements provided by the customer or regulatory requirements determined by the data classification.
b. BTS provides; advanced firewalls, role based access control, anti-malware, Intrusion detection, and patching of applications and operating systems to protect systems and data.
c. Software validation, modifications, and updates will be conducted by employees of the Medical Examiner and/or the Forensic Laboratory pursuant to the internal procedures of the Medical Examiner and Forensic Laboratory.
d. BTS personnel will not establish duplicated databases or files, extract data from database or files without notification to and approval of the Laboratory Director or Director of Investigations

4. Back up of Data

a. BTS will back-up all Medical Examiner and Forensic Laboratory applications and systems listed in Appendix A as provided by BTS back-up procedures.

5. Fault and Performance Monitoring

a. BTS monitors the Medical Examiner and Forensic Laboratory systems listed in Appendix A for best availability.
b. In the event BTS identifies a fault or performance issue; BTS will respond in accordance with the BTS Global Service Level Agreement utilizing the BTS Information Technology Infrastructure Library (ITIL) Service Management framework.

6. Access to Audit Reports

a. For systems in Appendix A that BTS is responsible for access control, BTS will maintain data in a manner that allows the Lab Director to receive, annually and upon request, an audit report detailing what users (inclusive of BTS, ME and PCFL staff) have access to the Medical Examiner and Forensic Lab data.
b. Audits and reports conducted per BTS procedures.

7. Breach Notification

a. BTS will notify the Director of the Forensic Laboratory or the Director of Investigations of any suspected intrusions, suspicious activity, or erratic behavior by administrator accounts, user accounts, or other internal or external entity.
b. BTS will take action and use the BTS Cyber Incident Response Team manual to minimize impact, contain, eradicate, recover and apply lessons learned to prevent future incidents.

c. All such security breaches will be documented. Documentation shall include an assessment of the impact of the breach. The Laboratory Director and the Director of Investigations shall receive a copy of the documentation.

8. Requirements for BTS Employee Access

a. Medical Examiner and Forensic Lab data and systems listed in Appendix A will be maintained by Criminal Justice Information Services (CJIS) (minimum level 2) certified staff and, consistent with ISO 17025:2005(E).
b. BTS access to systems listed in Appendix A shall be limited to staff with CJIS (minimum Level 2) clearance.
c. Documentation: report of who has access to data, report of staff members with CJIS certification, will be provided as necessary and/or required.
d. BTS employees will not provide data or access to data to any person or entity except as stated in these policies.
e. BTS employee requirements and access to Appendix A will be governed by BTS procedures.

Approval Date: _____

Effective Date: _____

Authorized By:

Signature: _____

Name: _____

Title: _____