COUNTY OF IMPERIAL
BOARD OF SUPERVISORS POLICY

Subject	Policy Number	Version	Page
DATA SECURITY POLICY	ITS-PO-004-2020	1.0	1 of 8

1. **Purpose**

The County of Imperial must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data leakage prevention.

2. Scope

2.1 In Scope

This data security policy applies to all customer data, personal data, or other data defined as confidential by the County of Imperial or any applicable State or federal law. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with County of Imperial ITS services is also subject to this policy.

2.2 Out of Scope

Information that is classified as Public is not subject to this policy. Other data that is not required to be kept confidential may be excluded from the policy by County of Imperial Chief Executive Office asked on specific business needs, such as that protecting the data is too costly or too complex.

3. Policy

3.1 Principles

The County of Imperial shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

3.2 General

a. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.

b. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.

c. Each user shall read this data security policy and the login and logoff guidelines, and sign a statement that they understand the conditions of access.

d. Records of user access may be used to provide evidence for security incident investigations.

e. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

3.3 Access Control Authorization

Access to County IT resources and services will be given through the provision of a unique user account and complex password. Accounts are provided by the Information and Technical Services department on the basis of records in the HR department.

Passwords are managed by the Information and Technical Services Department. Requirements for password length, complexity and expiration are stated in the *Password Construction Guidelines* policy.

Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

3.4 Network Access

a. All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.

b. All staff and contractors who have remote access to County networks shall be authenticated using the VPN authentication mechanism only. In addition Multi Factor Authentication is required as a secondary authentication mechanism for VPN connections.

c. Segregation of networks shall be implemented as recommended by County of Imperial network security research. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.

d. Network routing and firewall controls shall be implemented to support the access control policy.

3.5 User Responsibilities

a. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.

b. All users must keep their workplace clear of any sensitive or confidential information when they leave.

c. All users must keep their passwords confidential and not share them.

3.6 Application and Information Access

a. All County staff and contractors shall be granted access to the data and applications required for their job roles.

b. All County staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.

c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

3.7 Access to Confidential, Restricted information

a. Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.

b. The responsibility to implement access restrictions lies with the Information and Technical Services Department. Granular access to department data is to be defined by County of Imperial department heads and communicated to the Information and Technical Services Department for implementation.

4. Technical Guidelines

Access control methods to be used shall include:

- Auditing of attempts to log on to any device on the County network
- Windows NTFS permissions to files and folders
- Role-based access model
- Server access rights
- Firewall permissions
- Network zone and VLAN ACLs

- Web authentication rights
- Database access rights and ACLs
- Encryption at rest and in flight
- Network segregation

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

5. Reporting Requirements

This section describes the requirements for reporting incidents that happen.

a. Daily incident reports shall be produced and handled within the Information and Technical Services Department.

b. Weekly reports detailing incidents shall be produced by the Information and Technical Services Department and sent to the ITS manager.

c. High-priority incidents discovered by the Information and Technical Services Department shall be immediately escalated; the IT manager should be contacted as soon as possible.

d. The Information and Technical Services Department shall also product a monthly report showing the number of IT security incidents and the percentage that were resolved.

6. Ownership and Responsibilities

- **Data owners** are employees who have primary responsibility for maintaining information that they own, such as a department head or office manager.

- **Information Security Administrator** is an employee designated by the ITS management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.

- **Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.

- **The Incident Response Team** shall be chaired by the Chief Executive Officer and include employees from departments such as ITS, County Counsel, GSA, Auditors, and Human Resources.

7. Public Records

a. All messages, e-mails, voicemails, photographs, and other files stored on a County owned or leased computer hardware are generally considered public records, and are subject to disclosure under the California Public Records Act (Cal. Gov. Code §§ 6250 et seq.).

b. Any employee that has been granted access to County owned or leased computer hardware shall retain all records on the device in accordance with any applicable federal, State, or local records retention law or policy.

8. Enforcement

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection and/or contract terminated.

9. Definitions

This paragraph defines any technical terms used in this policy.

- **Access control list (ACL)** — A list of access control entries (ACEs) or rules. Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.

- **Database** — An organized collection of data, generally stored and accessed electronically from a computer system.

- **Encryption**—The process of encoding a message or other information so that only authorized parties can access it.

- **Firewall** — A way of isolating one network from another. Firewalls can be standalone systems or can be included in other devices, such as routers or servers.

- **Network segregation** — The separation of the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs.

- **Role-based access control (RBAC)** — A policy-neutral access-control mechanism defined around roles and privileges.

- **Server** — A computer program or a device that provides functionality for other programs or devices, called clients.

- **Virtual private network (VPN)** — A secure private network connection across a public network.

- **VLAN (virtual LAN)** — A logical grouping of devices in the same broadcast domain.

10. Related Documents

- Password Protection Policy

- Password Construction Guidelines Policy

- Acceptable Use Policy