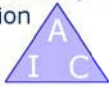




RIVERSIDE COUNTY

TELEWORK SECURITY STANDARD



PURPOSE3

SCOPE AND AUDIENCE.....3

TERMINOLOGY3

STANDARD3

GUIDELINES4

REFERENCE SECTION.....4

REVISION HISTORY4



PURPOSE

The purpose of this document is to define the Riverside County information security requirements for the implementation of Teleworking.

SCOPE AND AUDIENCE

All Departments implementing, managing and/or supporting any Telework capabilities for Riverside County.

TERMINOLOGY

Telework – a substitute for commuting in which work is moved to people instead of moving people to work.

Two factor authentication – something you know and something you have, such as a password and a token together.

Access Point – point of entry into the Riverside County network from a location that is external to the internal network infrastructure.

Authorized Department Designee – Department Head or person(s) assigned to authorize personnel to Telework.

Security Specification – implementation specific details that demonstrate conformance to all applicable security standards.

STANDARD

Listed below are the security requirements for Teleworking:

- Security specifications must be developed for all implementations and in turn be reviewed and approved by the ISO.
- Telework requests must be signed off by the Authorized Department Designee.
- Telework access points must meet Riverside County Perimeter Security Standard.
- If Telework access does not prevent the transfer of information (download, upload, etc.) then the remote computer system must comply with the Riverside County Computing Platform Security Standard which includes but is not limited to requiring:
 - Systems be actively managed and maintained to ensure:
 - Anti-virus is current and active
 - Security patches are current
 - Firewall is implemented to restrict all inbound access except management traffic

- Two factor authentication must be implemented.
- Sensitive information should not be stored on any device (laptop, desktop, PDA or other external data storage device) without an approved encryption solution.
- Telework access will be restricted to only the information and systems required to accomplish their job function.
- Telework access must prevent simultaneous access to non-County network resources.
- The remote session must be locked out after an idle-time of 10 minutes.
- Telework accounts must be evaluated and re-approved on an annual basis.
- Physical Security
 - Computer system must be located in an area that:
 - Prevents visual eavesdropping of private or confidential information
 - Prevents audible eavesdropping of private or confidential information
 - Printed Materials
 - Must be locked in storage cabinet
 - Must be disposed of in accordance with current Departmental standards

GUIDELINES

- N/A

REFERENCE SECTION

- N/A

REVISION HISTORY

Change Date	Changed by (Name)	Revision	Description of Changes	Approved By	Approval Date
08/28/08	Tom Plunkett	1.1	Final Document for Presentation to HR	Jack Miller	08/28/08