SECTION:	Information Technology	**POLICY #:**	705
TITLE:	Remote Access Control	**PROCEDURE #:**	705-A
		ORDER #:	19-114
DEPT:	Information Technology	**PROGRAM:**	Security
ADOPTED:	02/16 **REVIEWED:**	**REVISED:**	09/19

PURPOSE: The purpose of this policy is to authorize the Marion County Information Technology Department to develop, implement, utilize, and improve security and associated processes and procedures needed to enable remote access to county information technology resources.

AUTHORITY: The Marion County Board of Commissioners may establish rules and regulations in reference to managing the interest and business of the county under ORS 203.010, 203.035, 203.111, 203.230.

The Marion County Board of Commissioners expresses the governing body's official, organizational position on fundamental issues or specific repetitive situations through formally adopted, written policy statements. Policy statements serve to provide rules for public officials on the conduct of county business.

Marion County Administrative Policies and Procedures outline the forms and process through which the Board of Commissioners takes formal action on administrative policy. It is the official record of county administrative policy.

APPLICABILITY: All county departments.

GENERAL POLICY: Ensuring secure and reliable remote access to county information technology resources is an expectation of conducting county business. This policy establishes rules for the use and management of remote access capabilities.

DEFINITIONS:

Business Partner: A contractor whose services require access to county information technology resources.

Remote access: For purposes of this policy, remote access is defined as access to county information technology resources via secure internet-based applications including, but not limited to: secured tunnels, connection application, and client connections.

SUBJECT: REMOTE ACCESS CONTROL

POLICY GUIDELINES:

1. RESPONSIBILITIES
   - 1.1. County information technology (IT) resources may only be accessed remotely through capabilities implemented and maintained by the Marion County Information Technology Department (MCIT).
   - 1.2. It is the responsibility of MCIT to develop, own, and maintain processes and procedures defining creation, implementation, and ongoing support of remote access.
   - 1.3. It is recognized that some county IT resources may not be viable candidates for remote access due to technical constraints, security limitations, or agreed-upon business practices.
     - 1.3.1. A list of services for which remote access is available is maintained on the MCIT intranet page http://intra.co.marion.or.us/IT/
   - 1.4. A completed and signed remote access request form is required prior to issuance of a remote access account and password.
   - 1.5. Each department head is responsible for:
     - 1.5.1. Determining departmental use of supported remote access capabilities and determining the person(s) to whom remote access may be made available based on departmental business needs;
     - 1.5.2. Requesting remote access for authorized users via the MCIT Remote Access Request Process; and
     - 1.5.3. Ensuring that the use of remote access complies with personnel rules and collective bargaining agreements.
   - 1.6. Use of remote access shall comply with all county policies including but not limited to Administrative Policy 701, Use of Computing and Communications Assets.
   - 1.7. Remote access accounts and passwords may be used with:
     - 1.7.1. County-owned equipment;
     - 1.7.2. Personal equipment, such as mobile devices, used to perform limited county business functions as approved by the authorizing department head or elected official and MCIT; or
     - 1.7.3. Vendor-owned equipment for external parties having approval to connect to county-owned equipment as outlined in 1.9 and 1.10, below.
   - 1.8. Remote access may be requested for employees, volunteers, and external approved business partners on a one-time, intermittent, or ongoing basis depending upon business need.
     - 1.8.1. Duration of access should be requested only for the time needed to conduct county business remotely.
     - 1.8.2. To extend the remote access duration, a new request must be submitted.
   - 1.9. Remote access for external business partners typically occurs as a scheduled event under supervision of MCIT staff.
     - 1.9.1. An example of scheduled remote access is a collaborative work session between MCIT staff and a vendor representative for installation or upgrade of an application or other system resource.
   - 1.10. Ongoing and unsupervised remote access may be established under special circumstances to allow connection by authorized external parties to county-owned IT resources for completion of specific contractually-defined tasks supporting Marion County's operating environment when

scheduled remote access would delay delivery of services. For example, an after-hours triage and troubleshooting for vendors required to provide 24x7 services.

1.11. Activities performed via remote access shall comply with county policies, state ethics and elections laws, administrative rules, federal, state, and local law, as well as any signed contractual agreements with external parties.

1.12. Data created or maintained via remote access is subject to State of Oregon public records laws and retention schedules. Any data created and stored while accessing county IT resources via remote access is a public record.

1.13. Data created or maintained via remote access shall comply with county policies to ensure the confidentiality, integrity and availability of the data.

1.14. Violations

1.14.1. Proper use of remote access capabilities is the responsibility of all remote access users. Violation of this policy or its accompanying procedure may result in removal of remote access for specific individual(s), department(s), or business partners.

1.14.2. Violations may also be grounds for disciplinary action up to and including termination of county employment.

2. EXCEPTIONS

The chief administrative officer may authorize remote access in circumstances in which connectivity is needed for a specific period of time for a specific party performing work for the county under conditions not covered by this policy.

3. IMPLEMENTATION

The information technology director or designee is authorized to implement and execute this policy.

4. PERIODIC REVIEW

This policy shall be reviewed by the Information Technology Department at least every three years, or more often if needed, and updated as necessary.

Adopted: 02/16
Reviewed:
Revised: 09/19