SECTION:	**Information Technology**	**POLICY #:**	**705**
TITLE:	**Remote Access**	**PROCEDURE #:**	**705-A**
		ORDER #:	**16-23**
DEPT:	**Information Technology**	**DIVISION:**	**IT**
ADOPTED:	**02/16** **REVIEWED:**	**REVISED:**	

PURPOSE:

Marion County recognizes that remote access to internal county resources (i.e. corporate data, computer systems, networks, databases, etc.) is an essential tool through which authorized persons conduct county business in an approved, secure, and reliable manner. Remote access promotes effective and efficient service delivery and strengthens the county's ability to be responsive, accessible, and collaborative.

For purposes of this policy, remote access is defined as access to county resources via secure internet-based applications including, but not limited to:

- Secured tunnels (VPN, terminal services…)
- Connection application (Mobility, NetMotion…)
- Client connections (WebEx, GoToAssist…)

Technical fail safes are needed to ensure this access is protected from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to the county's public image. To this end, formal process and procedure will be developed for request, approval, and delivery of remote access capability.

This policy is being established to authorize Marion County Information Technology (IT) to develop, implement, utilize, and evolve the technical fail safes and associated processes and procedures needed to enable remote access while securing county 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 and 203.111.

The Marion County Board of Commissioners expresses the governing body's formal, organizational position of fundamental issues or specific repetitive situations through formally adopted, written policy statements. The policy statements serve as guides to decision making for both elected and appointed officials on the conduct of county business.

SUBJECT: REMOTE ACCESS POLICY

The Marion County Administrative Policies and Procedures manual of the Marion County Board of Commissioners outlines the forms and process through which the Board takes official action on administrative policy, and is the official record of county administrative policy.

APPLICABILITY: All county departments, employees, contractors, business partners, and volunteers.

GENERAL POLICY: The county has an overriding interest and expectation in deciding how to best ensure secure and reliable remote access to county resources. This policy establishes guidelines for use and management of remote access capabilities.

POLICY:

1. Responsibilities:

1.1. County resources may only be accessed remotely through capabilities implemented and maintained by Marion County IT.

1.2. Processes and procedures defining creation, implementation, and ongoing support of remote access will be developed, owned, and maintained by IT.

1.3. It is recognized that some county resources may not be viable candidates for remote access due to technical constraints, security limitations, or agreed-upon business practices. A list of services for which remote access is available will be maintained on the IT webpage.

1.4. Each department head or elected official is responsible for determining departmental use of supported remote access capabilities.

1.4.1. Each department head or elected official must determine the need for remote access and the person(s) to whom it may be made available based on departmental business needs.

1.4.2. Each department head, or elected official, will request remote access for authorized users via the IT Remote Access Request Process.

1.4.3. Use of remote access, as authorized by the requesting department head or elected official, must comply with personnel rules and collective bargaining units.

1.5. Use of remote access shall comply with all county policies and standards including but not limited to Administrative Policy 701: Use of Telephones, Computer and Data Communications Equipment, E-Mail and Internet.

1.6. Remote access accounts and temporary passwords will be created and disseminated to an authorized user by IT. The user must reset the temporary password upon initial use and may not share passwords with others.

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, to perform limited county business functions as approved by the authorizing department head or elected official and IT;
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 business partners on a one-time, intermittent, or ongoing basis depending upon business need. Duration of access should be requested only for the time needed to conduct county business remotely. To extend the remote access duration, a new request must be submitted.

1.9. Remote access for external business partners will normally occur as a scheduled event under supervision of MCIT staff who actively participate in the work session.

1.9.1. An example of scheduled remote access would be collaborative work sessions between MCIT staff and a vendor representative for installation or upgrade of an application or other system resource. Work would only be conducted in accordance with terms and conditions of an approved contract.
1.9.2. Access will be created via secure industry-standard connection tools including but not limited to GoToAssist or WebEx.
1.9.3. Access will be limited to the specific resource(s) for which the external party has service obligations.
1.9.4. Access events must be scheduled as appointments between the external party and an MCIT staff person having support responsibilities for the target resource(s).
1.9.5. The active remote session must be attended by an authorized MCIT staff person at all times.
1.9.6. The remote session must be terminated upon completion of the work. It must also be terminated if the session cannot be monitored by the MCIT staff person for any reason.
1.9.7. Once a party has been approved for scheduled remote access to perform a specific type of work, scheduled events may be executed between an authorized MCIT staff person and that individual or entity as needed.

1.10. Ongoing and unsupervised remote access may be created under special circumstances to allow connection by authorized external parties to county-owned resources. Ongoing remote access would be established for completion of specific contractually-defined tasks supporting Marion County's operating environment when scheduled remote access would delay delivery of services. An example would be after-hours triage and troubleshooting for vendors required to provide 24x7 services.

1.10.1. Access will be created via secure industry-standard connection tools including but not limited to Virtual Private Network (VPN).
1.10.2. Access must be requested by the department head or elected official having primary responsibility for the county resource being accessed. This access may be requested for an individual party or business entity with which the county is conducting official business
1.10.3. Once approved, access will remain in effect until withdrawn by the department head or elected official.
1.10.4. Withdrawal of access may be requested at any time and must be requested upon termination of contractually-defined services.
1.10.5. Access will be limited to the specific resource for which the external party has contractual support obligations.
1.10.6. Once approved, access sessions may be initiated by the external party upon identification of a critical service issue or to perform operational tasks as defined in an executed contract. Identification of a critical service issue may come through automated system alerts or communication of issues by Marion County staff.
1.10.7. The remote session must be terminated by the external party upon completion of the identified work.

1.11. Activities performed via remote access shall comply with county policies, state ethics and elections codes, and administrative rules. It shall also comply with 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 resources via remote access is a public record.

1.13. The county will approach the use of remote access capability as consistently as possible, enterprise-wide. To this end, requests for remote access will be submitted to IT by submitting a completed and signed Remote Access Request Form as described in the IT Remote Access Process and IT Remote Access Procedure documents prior to issuance of a remote access account and password.

To assess suitability of individual devices to be used to connect remotely, a separate Remote Access Request Form must be submitted for each device. A new Remote Access Request Form is required for use on alternate hardware.

Note: For remote access accounts pre-existing this policy, a Remote Access Request Form must be completed and submitted to IT for review and approval within 90 days of Board approval of this policy. Any non-compliant conditions will be reviewed by the department head or elected official and the IT Director to determine waivers or mitigations needed.

2. Exceptions:

Exception: Remote access may be granted by the IT Director 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.

Exception: For scheduled remote access (see Section 1.9, above), it is not necessary to submit a Remote Access Request Form for each device to be used once an individual or entity has been approved for this access in sessions actively managed by authorized MCIT staff.

3. Implementation:

The IT Director is authorized to implement and execute this policy via the Information Technology Remote Access Process and Procedure.

4. Violations:

The proper use of remote access enhances service delivery to internal and external county customers. It is the responsibility of county public officials to use this form of access properly. Violation of the policies or procedures set forth in this policy may result in removal of remote access for specific individual(s) or department(s). Violations may also be grounds for disciplinary action up to and including termination of county employment.

5. Periodic Review:

This policy will be reviewed by the Information Technology Director and County Legal Counsel every two years and updated as needed.

Adopted: 02/16

Marion County
OREGON

IT Process Description

Process Name: Remote Access Approval

Document Title	IT Process Description
Process	Remote Access Approval
Governance Sponsor	Tom Frey, IT Director
IT Leadership Sponsor	Julie Walton, IT Manager

Document Version

Indicate the major revisions of the document. Add rows as necessary.

Version	Status	Author	Reason for Version	Date
1.0	Original	J. Walton	Original Document	8/14/2015

Changes from Previous Version

Indicate the sections of the document that were revised for each version noted above and provide a brief description of the changes. Add rows as necessary.

Section	Description

Approval Signatures

By signing below, I agree that the process described in this document is approved for implementation by the Marion County IT Department.

Name	Role	Signature	Date
Tom Frey	Governance Sponsor		
Julie Walton	IT Management Sponsor		
Ken Pearson	IT Management Sponsor		

Table of Contents

1 Process Overview

This section provides high level information for the process.

1.1 Process Statement

This document describes the detailed task flow through which a Marion County department head or elected official requests remote access to county resources by Marion County employees, external business partners, and volunteers to perform approved work activities in accordance with the Remote Access Policy.

1.2 Definitions

Remote Access - Access provided to internal Marion County network resources or systems from a location or system outside of normal Marion County work locations.

Marion County Resource - Program or system to be accessed, for example email, P drive, or Intranet

1.3 Associated Policy, Procedure, and Other Supporting Documents

This process is defined under authority of 705: Remote Access Policy and 705A: Remote Access Procedure as approved by the Board of Commissioners.

To execute the 705A: Remote Access Procedure, the requestor and Information Technology (IT) will execute the Remote Access Approval Process maintained by IT.

As part of executing the Remote Access Approval Process, the requestor will complete portions of the Remote Access Request Form to identify the specific party for whom remote access is requested, the business purpose for which remote access will be used, and to acknowledge understanding of the security requirements associated with remote access. The party for who access is being requested will also review and sign the Acceptable Terms of Use portion of the Remote Access Request Form.

IT will complete those sections pertaining to assessment of compliance with policy and technical configuration. Should the request be business-necessary but non-compliant, IT and the requestor will jointly complete a waiver definition to identify points of non-compliance and mitigations taken to reduce risks associated with those points.

1.4 Process Review and Maintenance

This process will be reviewed at any of these junctures:

- Annually
- Upon significant change in the associated policy or procedure
- Upon changes in the Remote Access Request Form

2 Process Narrative

This section describes the steps required to execute the Remote Access Process in narrative format.

2.1 Need for Remote Access is Identified

A department identifies a need for one-time, periodic, or ongoing need for an employee, external business partner, or volunteer to access county resources via remote access to perform approved county business..

2.2 Remote Access Request Form is Completed by Requesting Department

A department requests remote access for staff, external business partner, or volunteer business partner by completing and submitting a Remote Access Request Form.

The requestor completes those sections identifying the person for whom remote access is being requested (may be the requestor or other party), the business purpose for remote access, the resources to be accessed, the equipment to be used, and other descriptive information needed to assess technical feasibility and compliance with the Remote Access Policy.

The person for whom remote access is being requested completes the section defining acceptable use to acknowledge understanding of how remote access is governed.

The requestor and person for whom access is being requested sign relevant areas of the form and submit the form to the department head or elected official as appropriate for that department.

2.3 Remote Access Request is Reviewed by Requesting Authority

The requesting department head or elected official reviews the Remote Access Request Form to ensure the access being requested meets departmental approval to ensure appropriateness of request.

If denied, the procedure ends. If approved, the requesting authority signs the Remote Access Request Form, and it is sent to IT as an attachment to a ticket.

2.4 IT Assesses Ticket

The ticket follows the standard IT intake process and is assessed to determine if additional information is needed to process the Remote Access Request Form. If sufficient information has been provided, the ticket is assigned to the Network Operations Queue for review by the Network Manager and work proceeds to Step 2.6.

2.5 IT Updates Ticket to Request Additional Information

The Service Desk updates the ticket to identify data needed to process the request. As this form must be signed by the authorizing department head or elected official, the requesting department must update the form and resubmit it. It is not permissible for IT to alter the form on behalf of the requesting department. Return to Step 2.2.

2.6 Remote Access Request is Reviewed for Compliance with Policy

The Network Manager and relevant IT staff review the request for compliance with established Remote Access Policy. If compliant, the Technical Requirements section of the checklist is completed to identify how remote access will be configured, the form is approved by the Network Manager, and work proceeds to Step 2.8..

2.7 Non-Compliant Conditions are Reviewed for Mitigation

If the remote access requested is not compliant, the Network Manager and technical staff work with the requesting department to identify options to allow the remote access request to gain compliance without compromising business requirements. Once the conditions of remote access have been modified to gain compliance, the Remote Access Request Form must be signed by the requesting department head or elected official to accept the revisions. (Return to Step 2.3).

If after review of options the request for remote access is unable to adhere to one or more policy requirements, the requesting department and Network Manager complete and sign the Waiver Request portion of the Remote Access Request Form with assistance from technical and business staff and business partner as needed. Both parties must sign the form, which is then attached to the ticket for routing to the IT Director for review.

2.8 Submission to IT Director for Approval

If the IT Director approves the request as signed, work proceeds with Step 2.10.

As an alternative, the IT Director may determine that any condition of non-compliance warrant further research for additional mitigations or that the request introduces undue risk and is denied. If further research is needed, the Network Manager and requesting department head or elected official proceed accordingly and resume the process at Step 2.2 with an updated request form.

2.9 Requesting Department Informed of Request Denial

If the remote access request is denied by the IT Director as it introduces undue risk to county resources, the requesting department head or elected official is notified by the IT Director as to the reasons for denial and the ticket is updated with this information and closed. Should the department head or elected official wish to submit a new request, the procedure begins with submission of a new request form and ticket. .

2.10 Implementation of Remote Access

Upon approval, Remote Access is created and configured in accordance with the approved Remote Access Request Form. The ticket is updated upon completion of work, and the final form is scanned and attached to the ticket. The hard-copy form is stored in the Remote Access Request Binder for three years.

3 Process Flow

This section describes the steps required to execute the Remote Access Process in diagram format.