TITLE: Remote Access Control		**PROCEDURE #:**	705-A
DEPT: Information Technology		**PROGRAM:**	IT Security
EFFECTIVE DATE: 02/16	**REVIEWED:**	**REVISED:**	09/19

OBJECTIVE: To establish a procedure for permitting remote access to county resources.

REFERENCE: Policy # 705

APPLICABILITY: All county departments.

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

PROCEDURES:

1. **Remote Access Request**
   - 1.1. When a department identifies the need for remote access for staff, a volunteer, or an approved business partner, the department must:
     - 1.1.1. Submit an MCIT ticket; and
     - 1.1.2. Complete and attach the remote access request form to the ticket.
   - 1.2. A separate remote access request form must be submitted for each device and alternate hardware.

2. **Assessment of Remote Access Request**
   - 2.1. Information technology staff shall review the request for compliance with Policy 705 then submit the form to the MCIT director or designee for review and approval.
   - 2.2. If the request is approved, the MCIT director or designee shall sign the form and submit it to the service desk for remote access deployment.
   - 2.3. If the request does not comply with Policy 705, MCIT staff will work with the requesting department to identify options for gaining compliance without compromising business requirements.
     - 2.3.1. If compliance can be gained, the request form must be revised and signed by the requesting department head and submitted to the MCIT director or designee for review and approval.
     - 2.3.2. If, after review of options, the request is unable to adhere to one or more policy requirements, the requestor and an MCIT manager shall complete a waiver request form with assistance from technical and business staff and business partner as needed.
     - 2.3.3. The completed and signed remote access request form and waiver request form must be submitted to the MCIT director or designee for review and consideration of the requested waiver.

2.4. If the MCIT director or designee determines that the request introduces undue risk, it may be denied and returned to the requesting department head with an explanation.
2.5. If the MCIT director or designee determines that any factor of a waiver request warrants further research or mitigation, the form is returned to the MCIT manager with an explanation. The process for determining compliance may be restarted.

3. Remote Access Deployed

3.1. Upon approval, MCIT staff must create and configure remote access in accordance with the approved request form.
3.2. Upon completion, MCIT staff will notify the requestor and authorizing department head that the request has been completed, and create and disseminated remote access accounts and temporary passwords to authorized user.
3.3. The user must reset the temporary password upon initial use and may not share passwords with others.
3.4. Access must be created via secure industry-standard connection tools including but not limited to virtual private network (VPN).

4. Employee and Volunteer Remote Access

4.1. The chief administrative officer, department heads, and MCIT Director may request withdrawal of remote access at any time.
4.2. Approved personal devices will not be supported by MCIT.

5. Supervised Remote Access for Business Partners

5.1. Work must be conducted in accordance with terms and conditions of an approved contract.
5.2. Remote access sessions for external business partners typically occur as a scheduled event under supervision of MCIT staff who shall actively participate in the event.
5.2.1. Access must be created via secure industry-standard connection tools approved by MCIT.
5.2.2. Access must be limited to the specific resource(s) for which the business partner has service obligations.
5.3. Remote access sessions must be scheduled as appointments between the business partner and MCIT.
5.3.1. Remote access sessions must be terminated upon completion of the work.
5.3.2. Remote access sessions must be terminated if for any reason, the access cannot be monitored by MCIT staff.
5.4. 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 as needed.

6. Ongoing Unsupervised Remote Access for Business Partners

6.1. The county may authorize unsupervised remote access through contracts with business partners.
6.2. The department head having primary responsibility for the county resource being accessed, must request access to conduct official business with a business partner.
6.2.1. Once approved, access will remain in effect until withdrawn by the department head.
6.3. Withdrawal of access may be requested at any time and must be requested upon termination of contractually-defined services.
6.4. Access is limited to the specific resource for which the business partner has contractual support obligations.

6.5. Once approved, access sessions may be initiated by the business partner u as defined in an executed contract.
6.6. The remote session must be terminated by the business partner upon completion of the identified work.

7. Scheduled Remote Access

7.1. 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 scheduled remote access in sessions actively managed by authorized MCIT staff.