
 <p>Cambridge Police Department</p>	POLICY & PROCEDURES		No. 211
	Subject/Title: Remote Access Device Usage Guidelines & Agreement		
	Issuing Authority: 		Review Date: March 5, 2012
	Robert C. Haas Police Commissioner		Issue Date: July 16, 2012 Effective Date: July 30, 2012 Rescinds:
References/ Attachments:		Accreditation Standards:	

I. PURPOSE:

The purpose of this policy is to define standards, procedures, and restrictions for connecting to Cambridge Police Department's internal network(s) or related technology resources via any means involving mobile devices, and personally owned remote access devices. This policy applies to, but is not limited to, all devices that fit the following device classifications:

- PC's running Windows, Mac OS, Linux and using any common internet browser.
- Smartphones running Android, BlackBerry OS, iOS, and Windows Phone 7.
- Personal internet connected devices with email capability (i.e. iPad, Kindle Fire, or any other tablet platforms).
- Devices that have integrated wireless capability. This capability may include, but is not limited to, Wi-Fi, Bluetooth, IR.
- Smartphones that include remote access device functionality.
- Any related components of Cambridge Police Department's technology infrastructure used to provide connectivity to the above.
- Any third-party hardware, software, processes, or services used to provide connectivity to the above.
- Any persons personal computer or mobile device used to connect to these resources.

The policy applies to any remote access device hardware and related software that could be used to access department resources, even if said equipment is not sanctioned, owned, or supplied by the Cambridge Police Department or the City of Cambridge.

II. POLICY:

It is the responsibility of any employee of the Cambridge Police Department who is connecting to the department's network via a remote access device to ensure that all components of his/her connection remain as secure as his/her network within the office. It is imperative that any wired (via sync cord, for example) or wireless connection, including, but not limited to remote access device and/or service, used to conduct department business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's remote access.

III. GENERAL GUIDELINES & CONSIDERATIONS:

The overriding goal of this policy is to protect Cambridge Police Department's technology-based resources (such as public safety data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of protected information, and damage to our public image. Therefore, all users employing remote access device-based technology to access police department technology resources must adhere to department-defined processes for doing so.

This policy applies to all department employees, including full- and part-time staff, contractors, freelancers, and other agents who utilize department-owned, personally-owned, or publicly-accessible remote access device-based technology to access the organization's data and networks via wired and wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at the Cambridge Police Department does not automatically guarantee the granting of these privileges.

Addition of new hardware, software, and/or related components to provide additional remote access device-related connectivity within corporate facilities will be managed at the sole discretion of the IT department. Non-sanctioned installations of remote access device-related hardware, software, and/or related components, or use of same within the department, or to gain access to organizational computing resources, are strictly forbidden.

All remote access devices and related connectivity points within the police department firewall will be centrally managed by the IT department and will utilize encryption and strong authentication measures. Although IT is not able to manage the public network to which wireless-enabled remote access devices and smartphones initially connect, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

IV. PROCEDURES:

- A. PDA Access & Usage Application:** Any member of the department wishing to have remote access to the department-owned network must complete an application (refer to *PDA Access & Usage Application* form). It is understood and agreed upon that when an employee makes an application for remote access to the department-owned network, said employee agrees to abide by and adhere to the procedural protocols established within this written directive. The application process will be followed as outlined:
1. The employee will fill out the application and submit the application to the Manager of the IT Department.
 2. Upon receipt of the completed application, the Manager of the IT Department will review the application and process the request.
 3. Once the application has been processed and remote access has been setup, the IT Department Manager will maintain a file on all such requests, returning a copy of the application for that employee's record, along with a copy of the instructions on how to gain remote access through his/her personal device (refer to attached copy of the *Instructions for PDA Access*).
- B. Use of Passwords:** Employees using remote access devices and related software to connect to the Cambridge Police Department's technology infrastructure will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with the department's password policy (as outlined below). Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
1. Users will be enrolled in an enhanced level of password security on their public safety domain account. This will result in the following list of password requirements:
 - a. Minimum of 8 characters;
 - b. Password must be changed every 90 days;
 - c. Cannot re-use an old password consecutively; and
 - d. After 10 failed logon attempts your account will be locked for 30 min before you can attempt to logon again.

- C. Use of Anti-Virus Protections:** All remote access devices that are used for business interests, whether personal- or city-owned, must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, power-on passwords. Any non-department computers used to synchronize with remote access devices will have installed whatever antivirus software deemed necessary by the department's IT department. Antivirus signature files must be updated in accordance with existing department policy.
- D. Protection of Passwords & Confidential Data:** Passwords and other confidential data as defined by the police department's IT department are not to be stored on remote access devices or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and related flash-based supplemental storage media.).
- E. Registration of PDA's IT:** Prior to initial use for connecting to the department's network, all remote access device-related hardware, software and related services must be registered with IT.
- F. Use of New Passwords:** Users must apply new passwords every business/personal trip where company data is being utilized on or synchronized to a remote access device.
- G. Authentication Requirements:** Any remote access device that is configured to access police department resources via wireless or wired connectivity must adhere to the authentication requirements of the police department's IT department. In addition, all hardware security configurations (personal or company-owned) must be approved by the police department's IT department.
- H. Modifications to Department-Owned Hardware/Software Prohibited:** Employees, contractors, and temporary staff will make no modifications of any kind to department-owned and installed hardware or software without the express approval of the police department's IT department. This includes, but is not limited to, installation of remote access device software on department-owned desktop or laptop computers, connection of sync cables and cradles to department-owned equipment, and use of department-owned wireless network bandwidth via these devices.

- I. Inventory of Approved Remote Access Devices:** The Cambridge Police Department will maintain a list of approved remote access device-specific software applications and utilities.
- J. Protection of Department-Owned Networks:** Employees, contractors, and temporary staff with police department-sanctioned wireless-enabled remote access devices must ensure that their computers and handheld devices are not connected to any other network while connected to the police department's network via remote access.
- K. Reporting Potential Security Compromises:** The remote access device-based user agrees to immediately report to his/her supervisor and the police department's IT department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.
- L. Monitoring of Access by PDA's:** The remote access device-based wireless access user also agrees to and accepts that his or her access and/or connection to the police department's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
- M. PDA's Not Subject to Reimbursements:** The Cambridge Police Department will not reimburse employees for business-related wireless remote access device-based access connections made on a pre-approved privately owned ISP service.
- N. Clarification of Policy:** It is the responsibility of any employee or other agent who may have remote access to the department-owned network to clarify any questions relating to this policy. Such clarifications should be directed to the police department's Manger of the IT Department.
- O. Right Reserved to Discontinue Access:** IT reserves the right to turn off without notice any access port to the network that puts the company's systems, data, users, and clients at risk.