Policy #10 - 01
Date Adopted:

Email Policy

Division of Criminal Justice Services

Approved By:
Francis X. Aumand III
For the VIBRS Advisory Board

Note: This is a *Mandatory* Policy.

1. GOALS

1.1. To establish an email policy that creates best practices on email usage, popping of email and transferring information to other email accounts without approval.

1.2. To appropriately manage the risk that various features such as internet access present to the integrity of the network and to the resources on the network.

1.3 To insure that the systems that provide network security are not bypassed.

2. POLICIES

2.1. The random, uncontrolled **forwarding or redirecting by rule of large quantities of DPS email** from an employee's departmental owned email account is strictly prohibited unless specifically authorized by the employee's department manager, or in the case of the Vermont State Police, the Staff Operations Officer or his/her designee.

2.2 Any manual forwarding of individual emails outside of the VIBRS network, without permission, that contains personal identifiable information (name, DOB, address etc.) is prohibited.

2.2.1 This policy is not intended to prohibit the selected individual forwarding of email or groups of email, where the employee is making an informed decision to forward the specific email or group of email at the time the forwarding is being done.

EXAMPLE:
DPS users that use DPS IT resources shall not; except as provided in the Policy Statement, forward all their DPS email from their DPS account to a non-DPS account. An example of this is Jane Smith, shall not create a rule in her email client that automatically forwards her DPS email to an outside account.

2.3 POP connections external to the VIBRS network will not be allowed.

3. DEFINITIONS

31 **POP PROTOCOL** – Post Office Protocol is a standard internet protocol used to retrieve email from a remote server to an end user PC utilizing a standard TCP/IP connection.

3.2 **MALWARE** - Short for ***mal****icious soft****ware***, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

3.3 **MAIL GATEWAY** – A server whose function is to protect network resources from malware by examining each message for proper content. The network is designed to route all supported mail through the gateway, thereby insuring protection.

3.4 **BLOCKING** – An automated function that disallows certain events from occurring. Examples: 1.) file sharing can be blocked between sites, 2.) general access into the VIBRS intranet is blocked.

4. E-mail Generally

4.1. E-mail sent to an individual user is not to be considered "Confidential." However, no one should look at another person's e-mail unless they have permission from that user or the person is the user's supervisor and the supervisor has cause within the limits of his/her supervisory authority.

4.2. E-mail groups are subject to change without notice. If you must be certain of the recipients of an e-mail message, do not use an e-mail group. E-mail that is sent to an e-mail group should be considered the same as a posting on a bulletin board.

4.3. The e-mail system is for the use of VIBRS users with the following restrictions:

4.3.1. Offensive material is not allowed.

4.3.2 Users shall restrict the use of e-mail to official business as determined by their agency head. These restrictions shall include but not be limited to;

3.3.2.1 Lobbying public officials or asking others to lobby in their behalf.

4.3.2.2 Printing and/or distributing information from the Internet that is obscene, potentially offensive, harassing or disruptive.

4.3.2.3 Using or allowing others to use Internet services or e-mail accounts to conduct transactions or advertising for a personal profit making business.

4.3.3. Users shall take reasonable measures to limit the amount of e-mail they generate.

4.3.4. Users should be aware that system backups would contain copies of e-mail messages. Deletion of an e-mail message does not guarantee that all copies of the message have been erased.

4.3.5. Users should be aware that the contents of e-mail could be used as evidence in civil, criminal and internal investigations. Therefore, e-mail should not contain any material, which can be construed to indicate bias, prejudice or any other litigation liability, which may be damaging to the departments that use the VIBRS network.

4.3.6 Users should never include their password or any other security related information in an e-mail message.

4.3.7 No employee shall send e-mail that is, or appears to be, sent from another employee's e-mail or that attempts to mask identity.

5.0 **Pop Email**

5.1 Email shall be automatically examined for any malware prior to being opened on any system.

5.2 All supported email will be routed through a mail gateway to detect malware prior to delivery.

5.3 As a general rule, CJS IT staff will block POP connections external to the VIBRS network.

5.4 User agencies that are part of the centrally managed anti-virus program can request POP connections for legitimate uses. Requests for POP access will go through the local Tech liaisons to the DPS/CJS IT staff. Tech liaison requests must have the authorization of the agency head and DPS/CJS IT staff will treat a request as if it has come from the agency head.

5.5 Tech liaisons will insure that PCs with authorization to POP mail are being managed by the central anti-virus program and that the anti-virus application is functioning properly.