Policy #05-01 Date Adopted: **4/6/2005**	**Popping of Mail from Outside the VIBRS Network** **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 a policy that provides guidance to all users and technical contacts concerning the use of mail clients that use the POP protocol for contacting external systems.

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. **DEFINITIONS**

2.1 **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.

2.2 **MALWARE** - Short for malicious software, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

2.3 **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.

2.4 **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.

3. **STANDARD / PROCEDURES**

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

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

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

3.4 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.

3.5 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.