Montgomery County Government
Department of Information Systems and Telecommunications
Internet, Intranet, & Electronic Mail Policy

I. PURPOSE

This material sets forth Montgomery County's policy (hereafter referred to as "the Policy") for proper use of Internet, intranet, and Electronic Mail (E-Mail) access provided by the County.

The Internet, intranet, and E-Mail connection and services are provided for employees and persons legitimately affiliated with the County for the efficient exchange of information and the completion of assigned responsibilities that are consistent with the County's statutory purposes. Violation of the Policy is prohibited and may lead to disciplinary action and dismissal.

II. APPLICABILITY

The provisions of this policy apply to all employees and contractors of the County, as well as approved affiliates, organizations or persons. This includes full-time, part-time and temporary employees using Internet, intranet, and E-Mail systems provided by the County.

III. RESPONSIBILITY

The following are the responsibilities of the participants in the County's Internet, intranet, and Electronic-Mail activities:

A. DEPARTMENT OF INFORMATION SYSTEMS & TELECOMMUNICATIONS (DIST)

DIST will provide a 24-hour, 7 day-a-week secure centralized connection to the Internet, intranet, and to Electronic Mail. The Internet and intranet service will allow County PCs to connect to the Internet and intranet via a high-speed telecommunications link while being simultaneously connected to the County's computer network backbone.

DIST will develop and maintain the Policy. This policy will be designed to protect the County's computer networks and data assets against unauthorized and malicious use, as well as to prevent potential misuse of County resource. DIST will maintain Internet and intranet security and maintain it on the firewall.

DIST will approve/disapprove any connections to the Electronic Mail system and to the Internet and intranet via the County's centralized connection. Any alternative means of connection proposed by the departments and agencies must be approved in advance by DIST.

DIST will maintain the County's World Wide Web Server and approve any web pages connectivity and architecture. DIST will maintain the web server platform, and will approve/disapprove any alternate web site platforms proposed by the departments and agencies.

DIST will connect the County's Enterprise E-Mail system to Internet mail in such a way that mail can be transacted between these systems without manual intervention. DIST will establish, publish and maintain E-Mail naming standards and conventions in support of the E-Mail connection.

DIST will maintain the current version of the Policy on an Electronic Bulletin Board.

The DIST Help Desk will take support calls when a problem is noted and will distribute information, updates, and/or resolutions as appropriate. The DIST Help Desk will log problems, resolutions, etc., and will issue E-Mail and Voice Mail messages when outages occur.

B. OFFICE OF HUMAN RESOURCES (OHR)

OHR will offer Internet and Electronic Mail training programs for County employees. These programs will cover the County's Internet, intranet, & Electronic Mail policies and procedures as well as etiquette, acceptable practices, and resources.

C. OFFICE OF PUBLIC INFORMATION (OPI)

The OPI will oversee the design of the County's web site and all subsequent additions/changes to it. The OPI will maintain and enforce a procedure for the departments and agencies to submit requests for the placement of information and web pages consistent with the County's standards for the publishing and maintenance of County web pages. The OPI will approve any web pages housed on the County's World-Wide Web Server and will monitor, audit and enforce information management standards on updates to web pages on the County's web site.

D. DEPARTMENTS AND AGENCIES

Department and agency heads or their designees must approve the use of the Internet by each department's employees on an individual basis.

Departments and agencies will be responsible for the enforcement of the County's Internet, intranet, & Electronic Mail security and use policies. Department and agency heads will take remedial action (including any disciplinary action they deem appropriate) when their employees do not adhere to the Policy.

The departments and agencies will fund for and arrange with the OHR or other resource to provide Internet and E-Mail training to all employees that will be required to access these systems. The departments and agencies will be responsible for making a copy of the latest Policy available to its employees as an integral part of this training.

The departments and agencies will be responsible for the design, development, and funding of their web pages. The departments and agencies will coordinate and submit requests for the establishment of their web pages to the OPI. The departments and agencies will obtain OPI and DIST approval prior to embarking on the establishment of a web site on other than the County's web server.

All departments intending to have their employees access the Internet and intranet must install anti-virus software on their PC's and network servers prior to such use. This software must be able to detect and eliminate viruses. This software must be kept up-to-date by each department with the most recent vendor-supplied viral signatures. Any viruses that are detected must be isolated, promptly reported to DIST, and then eradicated by the department.

All departments must submit requests for alternative Internet connections in writing to DIST for approval. All departments must submit alternative website, server, domain names, etc. in writing to DIST for approval.

Each department's technical staff will be responsible for receiving and resolving complaints or problems. Technical staff members will work with DIST staff for assistance and consultation when additional support is needed.

E. COUNTY EMPLOYEES

County employees must adhere to the Policy and are responsible for having the latest version of the policy. Employees must maintain security in accordance with the County's Office Automation Security Policy in using the Internet, intranet, and Electronic Mail. If potential risk is known to exist in any Internet, intranet, or E-Mail activity, employees must discontinue/discourage such activity and immediately report it to their supervisor, technical support staff or DIST.

IV. OWNERSHIP

All electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of Internet, intranet, or E-Mail are the property of the County. All electronic communications generated by employees of the County or stored on County equipment are the property of the County and, therefore, are not considered private. They may be retrieved from storage by the County and its agents, even though they have been deleted by the sender and receiver. These messages may be used in disciplinary proceedings.

V. POLICY

Internet and intranet connection must only be made in the following manner:

- With DIST approval, PCs connected to the County's computer networks may connect to the Internet and intranet via the County's secure Centralized Internet Service connection.
- Stand-alone (non network-connected) PCs may be used to dial into the Internet and intranet. Connections to the Internet through services, such as America On-Line or Compuserve, are authorized only from a stand-alone PC. Stand-alone PC's connecting to the Internet should have anti-virus software active on them. If a stand-alone PC is to be connected to the County's computer networks after it has been in Internet service, then the using department must check the entire data contents of the PC for viruses before connecting to the network (see section on Responsibility above).

Use of the Internet, intranet and Electronic Mail and their related resources is designated for County business.

Employees are prohibited from using the County's Internet and intranet connections or E-Mail for private gain or profit. Although the personal use of County Internet, intranet and e-mail resources is discouraged, the County recognizes that circumstances sometimes arise which necessitate personal use. Employees must keep personal use of these resources to a minimum so it does not disrupt their job performance. The County may discipline employees whose personal use of County Internet, intranet and e-mail resources disrupts their job performance or is otherwise inappropriate or excessive.

Employees may not use the County's Internet and intranet connections (including E-Mail and web pages) to give out personal or unofficial opinions.

Employees responsible for web page design will ensure that the County's Internet and intranet web pages designed by them reflect only official County information and do not point to sites not authorized by the Public Information Office (OPI). Such employees will also cooperate with the OPI in the review of web pages designed by them before they are made available on the Internet and intranet, .

Introduction of viruses or other software via the Internet or intranet that may disrupt the normal functioning or impair the capacity of the County's computers, data bases and computer networks is prohibited.

Employees whose PCs are enabled to accept files via the Internet (e.g., via FTP, E-Mail attachments, newsgroups) are individually and directly responsible for checking them for viruses using the latest version of a reliable virus checking program. Any viruses that are detected must be kept isolated by the department until DIST is notified and the virus is successfully eliminated. As a minimum, any PC on which a virus is detected must be immediately disconnected from the County network.

Unauthorized or malicious entry into the County's Internet and intranet connections or E-Mail or their associated security mechanisms is prohibited as are attempts to circumvent or defeat such protection mechanisms.

Employees shall not post, display or make easily available any access information, including, but not limited to, passwords. Employees shall not share an E-Mail password, provide E-Mail access to an unauthorized user, or access another user's E-Mailbox without authorization.

Employees or vendors responsible for connecting non-County networks to the County's networks must ensure that any networks to which the County network is being connected are not linked to the Internet or intranet without adequate firewall protection. DIST must be notified prior to connecting the non-County and County networks.

Employees must not violate the privacy of others and must be sensitive to the shared nature of the County's Internet and intranet facilities and the public nature of the Internet and intranet itself.

Those employees using the County's centralized connection to access either the Internet, intranet, or E-Mail must abide by all procedures discussed in the Internet or Electronic Mail training sessions.

Employees will not display any information on the Internet that is not of a public nature.

Costs incurred by employees in their use of the Internet and intranet must be in accordance with their department's policy and must be previously approved by their department.

Employees must use the Internet, intranet, and E-Mail in accordance with all applicable laws and regulations.

- Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the County's policies concerning "Equal Employment Opportunity"; and "Sexual Harassment and Other Unlawful Harassment."
- County employees must not create unusual mail routing and distribution patterns, including issuing global broadcasts, on the Internet.. Messages sent to all E-Mail users require prior approval by an appropriate member of the County.
- Use of the County's Internet or intranet connections to gain unauthorized access to resources via the Internet or intranet is prohibited.
- Programs and data protected by copyright and license laws must not be infringed upon by County employees.

The County reserves the right to monitor its E-Mail system - including an employee's mailbox - at its discretion in the ordinary course of business. Please note that in certain situations, the County may be compelled to access and disclose messages sent over its E-Mail system. The Maryland Public Information Act (MPIA), Maryland Code Ann., State Gov't §§ 10-611 to 10-628 (1993 Repl. Vol.) applies to an electronically stored E-Mail message or a hard copy of the message in the custody and control of a public officer or employee, if the message is related to the conduct of public business. 81 Op. Att'y Gen __, Op No. 96-016, 1996 WL 305985 (1996).

The systems administrator can access an employee's e-mail, as well as computer files related to an employee's Internet and intranet use, even though the employee use a privately held password to access their computer and e-mail. The existence of passwords and "message delete" functions do not restrict or eliminate the County's ability or right to access electronic communications.

Supervisors may access employee e-mail and computer files related to an employee's Internet and intranet use when there is a legitimate business need (i.e., a noninvestigatory work-related intrusion or an investigatory search for evidence of suspected work-related misfeasance).

The employee's use of the Internet, intranet and e-mail system indicates consent to the employer's review of his or her electronically stored e-mail and computer files related to the employee's Internet and intranet use.

Any employee who violates this policy shall be subject to disciplinary action.