

## **INTERNET USE GUIDELINES**

The Internet represents a value-added working tool that offers great benefits to its users and to the city. Unfortunately, Internet access can also divert attention from productive work practices and heighten security risks. Inappropriate use of Internet resources can also increase the city's exposure to liability and make city networks more vulnerable to hackers, virus infections, and other dangers.

Departments should make all Internet users aware of the following specific guidelines. Users must understand the potential liability and security risks associated with use of City equipment to access the Internet. The following guidelines represent "best-practices" that will help to ensure appropriate Internet use so as to avoid exposing individual employees, the department and the city to undue risks.

State law, federal laws, regulations and legal decisions, City of Milwaukee Ordinances and Information Security Policies provide the basis for many of the following guidelines. Consequently, departments are strongly encouraged either to adopt the guidelines as written or to use the guidelines as the basis for developing department-specific policy statements.

- 1. AUTHORIZATION:** City department managers will determine whether Internet access is consistent with the duties of and will enhance the productivity of an employee. Departments should routinely review employee access privileges to determine if the employee has used the resource effectively and whether continued access to Internet is warranted.
- 2. ACCESS:** Authorized users connected to the City's Wide Area Network will receive Internet access privileges. Employees who do not receive access to the Internet as part of their official duties should not be allowed to access the Internet using another employee's account and equipment. When an employee assumes a new position or responsibilities, the department should review his or her Internet authorization to determine the need for continued access. Access terminations are accomplished by departmental notification to their respective city Internet service provider.
- 3. OFFICIAL USE:** The City of Milwaukee encourages its employees to use the Internet for work-related research, to provide services to citizens, and for any other activity that supports the City's mission. City departments may also choose to authorize limited incidental use of the city's Internet resources for personal purposes as deemed appropriate. However, departments must ensure that such use does not impair the employee's ability to fulfill his or her job responsibilities and does not impose any additional costs or liabilities on the city. Under no circumstances should employees be permitted to use city equipment and Internet access for illegal activities, profit-making ventures or political endeavors. Departments should also prohibit use of city resources for playing games against opponents over the Internet. The Information and Technology Management Division of DOA, if requested, can assist departments in monitoring employee use of Internet resources with tracking software.
- 4. VIRUSES:** Virus infection represents one of the most well-documented threats of Internet use. Employees must scan all incoming files for viruses, whether downloaded or attached to electronic mail messages. Users should not open or attempt to read any files received over the Internet that they did not specifically request, and should immediately contact their network administrator upon receiving an unrequested file.

- 5. COPYRIGHT:** Information placed on the Internet is the intellectual property of the person or organization posting it. Users must be sure to cite their sources when using any text, ideas, software, or graphics copied from the Internet.
- 6. CITY PROPERTY:** All Internet transmissions sent from or received through City computers are considered City property. City and departmental management reserve the right to examine, at any time and without prior notice, all directories; downloaded text, image, audio and video files; and other information (business-related or personnel) stored on data disks, computers, and/or other media.
- 7. PUBLIC RECORD REQUESTS:** Requests from outside the City for access to electronic files should be handled through the same procedures as requests for any other public record. Thus, employees should not send out files containing city information without prior approval of the department manager.
- 8. SECURITY:** Employees may not deliberately propagate any virus, worm, Trojan horse, or other program code that interferes with or degrades operation of the city's computer systems or systems of another entity. Likewise, users may not deliberately expose systems of the city or other entities to risk nor use city systems to attempt unauthorized entry into secure areas of the city system or similar areas of other non-city systems.
- 9. FEE RESOURCES:** Access to some resources requires payment of an additional fee. Department managers may want to require that staff seek prior approval for access to any fee-based Internet resources.
- 10. FILE TRANSFERS:** Large file transfers should be done at times when they will not significantly degrade the performance of the City network. Non-peak network hours are from 6:00 p.m. to 8:00 a.m. weekdays and any time on Saturday or Sunday.
- 11. DISCUSSION GROUPS:** The Internet contains numerous discussion groups or forums where users may post messages and exchange ideas. Many of these are useful places for research on topics of interest to City departments. However, users may not knowingly misrepresent themselves or their employment by the city; they must always identify themselves honestly, accurately, and completely. As with any other form of communication, departments are responsible for any misrepresentation of official City policy made by employees and posted to the Internet. Department managers may want to require prior approval for employees to post messages to such locations.
- 12. RESPONSIBILITIES:** The City of Milwaukee trusts that its employees will act responsibly, and always in the best interests of the taxpayers who support them and the customers who depend on them. Each individual is responsible for complying with all applicable state and federal laws, and all City policies and standards when using City equipment to access the Internet. City departments will be held accountable for the actions of individual employees to ensure that conduct meets guidelines established for appropriate use of Internet.
- 13.** The city will establish any and all policies necessary and monitor operations to protect employees from creating legal liabilities and negative publicity for themselves and the city. Violations of any policies or standards can result in disciplinary action against the employee in accordance with local, state, and federal law and City administrative rules. Persistent abuse

of Internet access by City employees can result in permanent revocation of Internet privileges for the person or persons involved.