University of Massachusetts Global

Technology Use Policy

April 2021

Table of Contents

Executive Summary

This document covers the Technology Use Policy for the University of Massachusetts Global ("UMass Global"), a nonprofit affiliate of the University of Massachusetts. This policy outlines who the policy is for and what it covers.

Introduction

This policy applies to all employees, students, contractors, visitors, affiliates and any other user (collectively known as "users") that connects to UMass Global's Network or uses the Technology or Technology Infrastructure provided and maintained by UMass Global.

Policy Summary

UMass Global provides various Technology Resources to authorized users to assist them in performing their job duties for UMass Global. Each user has a responsibility to use UMass Global's Technology Resources in a manner that increases productivity, enhances UMass Global's public image, and is respectful of other UMass Global users.

Failure to follow UMass Global's policies regarding its Technology Resources may lead to disciplinary measures, up to and including termination for employees. For students and contractors this may involve a termination of their relationship with UMass Global. In addition legal proceedings may be entered into, taking into account the scope of the violation, and any possible adverse impact to UMass Global.

"Technology Resources" consist of all electronic devices, software, and means of electronic communication, including but not limited to, the following, whether provided or supported by UMass Global:

- personal computers and workstations;
- laptop computers; servers;
- computer hardware, such as wireless devices and network components;
- peripheral equipment, such as printers, scanners, fax machines, and copiers;
- computer software applications and associated files and data, including software that grants access to external services, such as the Internet; electronic mail; telecommunications systems such as telephones; cellular phones; smart phones; pagers; personal digital assistant devices, messengers and voicemail and text mail systems.

Users have no right of privacy with respect to any information or messages – including personal information or messages – created, received or maintained on UMass Global's Technology Resources.

Acceptable Uses

UMass Global's Technology Resources are to be used by users only for the purpose of conducting UMass Global business. Users may, however, use UMass Global's Technology Resources for incidental personal uses so long as such use does not interfere with the user's duties, is not done for pecuniary gain, does not conflict with UMass Global business and does not violate any law or UMass Global policy.

Personal data or transmissions using UMass Global Technology Resources are not subject to the same protections as UMass Global data and transmissions. UMass Global assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on its Technology Resources. UMass Global strongly discourages users from storing any personal data on any of UMass Global's Technology Resources.

Improper Uses

Under no circumstances may users use UMass Global's Technology Resources to transmit, receive, or store any information that is discriminatory, harassing, or defamatory in any way (e.g., sexually-explicit or racial messages, jokes or cartoons), or to violate UMass Global's Policy Against Harassment.

Users must not use UMass Global's Technology Resources to copy, retrieve, forward or send copyrighted materials unless the user has the author's permission or is accessing a single copy only for the user's reference.

Users may not use any of UMass Global's Technology Resources for any illegal purpose, violation of any UMass Global policy, in a manner contrary to the best interests of UMass Global, in any way that discloses confidential or proprietary information of UMass Global or third parties, or for personal or pecuniary gain.

UMass Global Access to Technology Resources

All messages sent and received, including personal messages and all data and information stored on UMass Global's electronic-mail system, voicemail system or other computer systems/resources are UMass Global property regardless of the content. As such, UMass Global reserves the right to access all of its Technology Resources including its computers, voicemail and electronic-mail and text-mail systems, at any time, in its sole discretion.

Although UMass Global does not wish to examine personal information of its users, on occasion it may need to access any and all information in its Technology Resources, including but not limited to: computer files, electronic-mail messages, text messages, social media posts, messenger communications and voicemail messages.

Passwords

Most of UMass Global's Technology Resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. Passwords do not confer any right of privacy upon any user. Thus, even though users may maintain passwords for accessing Technology Resources, users must not expect that any information maintained on UMass Global's Technology Resources, including but not limited to: text, electronic-mail and voicemail messages, may be maintained in private.

Users must not share their passwords and must not access any other user's system(s) without express authorization from UMass Global.

Two-Factor Authentication

UMass Global has implemented two-factor authentication across certain key systems. This allows a code to be sent to the user. The user may not share this code with anyone as it may compromise the confidentiality, integrity and availability of UMass Global's Technology Resources and information.

Data Collection By UMass Global

The best way to guarantee the privacy of personal information is not to store or transmit it on UMass Global Technology Resources. To ensure that users understand the extent to which information is collected and stored, below are examples of information currently maintained by UMass Global. UMass Global may, however, in its sole discretion, and at any time, alter the amount, the type of information that it retains and the retention period of said information.

Telephone Use and Voicemail
Records are kept of all calls made from and to a given telephone extension. Although voicemail is password protected, an authorized administrator can reset the password and listen to voicemail messages.

Electronic Mail
Electronic mail is backed-up and archived. Although electronic mail is password protected, an authorized administrator can reset the password and read electronic mail.

Desktop Facsimile Use
Copies of all facsimile transmissions sent and received are maintained in the facsimile server.

Document Use
Each document stored on UMass Global computers has a history, which shows which users have accessed the document for any purpose.

Internet Use
Internet sites visited, the number of times visited, and the total time connected to each site is recorded and periodically monitored, as allowed by applicable law.

Backups
UMass Global maintains backups of its information which may be restored and reviewed at any point in time at the University's discretion.

Cell Phones
Information maintained on UMass Global provided cell phones may be subject to review at any point in time.

Deleting or erasing information, documents, or messages maintained on the UMass Global's Technology Resources is, in most cases, ineffective.

Internet and Electronic Mail (Including Text Messages)

UMass Global expects that when users use the Internet or electronic mail during work hours, while on UMass Global premises, or remotely through the use of UMass Global computer equipment, they will do so in a responsible manner, and for work-related purposes only. UMass Global expects users to exercise discretion and good judgment when accessing the Internet and when sending or receiving electronic mail and attachments thereto.

Social Media

UMass Global maintains a social media presence and may review social media for mentions of UMass Global to determine the public perception of UMass Global life and services. We ask that any user posting information about UMass Global ensures that it

- is not confidential and/or privileged information,
- does not adversely impact UMass Global.

UMass Global may ask its employees, contractors, or students to remove social media posts that do not comply with the above stated principles. Refusal to do so may result in the termination of their relationship with UMass Global. In addition, any libelous posts may lead to legal proceedings against the individual.

Personal Electronics Policy

Users must devote their full time, energy and attention at work to their job responsibilities and duties. For purposes of personal listening, use of personal electronic devices such as cell phones, iPods, radios, CD players, MP3 players or similar personal entertainment technologies are allowed only when it is not a distraction to the user or others around them. UMass Global retains the right to prohibit use of such personal devices in its sole discretion. UMass Global reserves the right to prohibit the use of UMass Global Technology Resources for personal purposes, including access

to internet radio services, video services, any streaming services, games or any other areas, as determined by UMass Global.

A user's use of their personal cell phone for personal calls is permissible during meal, and rest periods (not counting emergencies). Personal cell phones must remain in a quiet or vibrate mode during working hours. Excessive use of personal cell phones during work hours is not permissible and may lead to discipline, up to and including termination for employees. For contractors, visitors and students, this may involve a termination of their relationship with UMass Global.

Use of UMass Global Property and Inspections

Damages

All UMass Global property, including but not limited to desks, storage areas, work areas, file cabinets, files and machines are provided for UMass Global use only and must be used properly and maintained in good working order. Employees must immediately notify their supervisor if UMass Global property appears to be damaged, defective, or in need of repair. Employees who steal or misuse company property may be personally liable for replacing or fixing the item and may be subject to discipline, up to and including termination. For contractors, visitors and students, this may involve a termination of their relationship with UMass Global. In addition legal proceedings may be entered into, taking into account the scope of any physical or digital damage and any additional, possible adverse impact to UMass Global.

Inspections

UMass Global reserves the right, at all times and without prior notice, to inspect and search any and all of its property for the purpose of determining whether this policy or any other UMass Global policy has been violated, when an inspection is necessary for the purposes of promoting safety in the workplace or compliance with State and Federal laws, or for any other legitimate business reason. These inspections may be conducted during or after business hours and in the presence or absence of the employee.

Security Search

In order to ensure the safety and security of employees, students, contractors, visitors and any other individuals at UMass Global, and to protect UMass Global's legitimate business interests, UMass Global reserves the right to question and inspect or search any employee or other individual entering onto or leaving UMass Global premises. The inspection or search may include any packages or items that the individual may be carrying, including briefcases, handbags, knapsacks, shopping bags, et cetera. These items are subject to inspection and search at any time, with or without prior notice. Refusal to cooperate with a request to submit to a search may cause disciplinary action, up to and including termination for employees. For contractors, visitors and students, this may involve a termination of their relationship with UMass Global. For the purposes of inspecting, investigating, or searching employees', contractors', students' or visitors', files or documents, UMass Global may override any applicable passwords, codes, or locks.

Usage of Cellular Phones and Wireless Devices

Certain States, including California, prohibit the use of wireless phones by drivers operating motor vehicles, unless the phone being used is specifically configured for hands-free use, and also prohibit texting while driving. Users who must drive as part of their job duties and who are required to use wireless phones to conduct business may be issued hands-free devices for the wireless phones. However, users are strictly prohibited from using wireless phones, including hands-free devices, while operating a UMass Global vehicle or their own vehicle during working time unless they are able to do so legally and safely.

A user who is charged with traffic violations resulting from the use of a cellular telephone or other wireless device while driving will be responsible for all liabilities that result from such action.

Users may use UMass Global-provided cellular telephones or other wireless devices for incidental personal use only. Users should take care to use proper business etiquette when representing UMass Global and using a cellular telephone or wireless device. Cell phone invoices will be regularly monitored, and text messages may be reviewed.

Copyrighted Material

Plagiarism and the unauthorized use of copyrighted material are strictly prohibited by UMass Global. Users may not use UMass Global Technology Resources to violate this principle.

Cyber Security Awareness Training

At its discretion, UMass Global arranges for Cyber Security Awareness Training for its user community (or a sub-set of the user community). Any communications instructing the end user to take part in Cyber Security Awareness Training and any associated activities must be followed as this training and any associated activities are mandatory.

Phishing Tests

Phishing Tests are conducted at UMass Global's discretion to improve Phishing awareness in its users. Users who are found to be susceptible to Phishing e-mails as a result of the test will be required to take mandatory Phishing Awareness Trainings in addition to any previously assigned training by UMass Global.

Information Security Incidents

Information Security at UMass Global is concerned with the Confidentiality, Integrity and Availability of UMass Global Technology Resources and Information. Any Information Security concern, risk or gap (as identified above) should immediately be brought to the attention of the UMass Global Service Desk.

Tampering

Tampering with UMass Global-owned Technology Resources, including but not limited to cell phones, is considered to be making unauthorized changes to the hardware or software that may be in conflict with licensing agreements or may void applicable warranties. Users must not perform such changes unless they are explicitly authorized by UMass Global.

Working From Home

During the period of the Coronavirus Pandemic, UMass Global has implemented Work From Home policies. This means that the end user is responsible for ensuring responsible precautions for Information Security and Health related reasons, some of which are outlined below. Please follow local and federal laws, guidelines and best-practices in your area in addition to what has been outlined below:

Lock Your Devices
End users must ensure that their Technology Resources (Tablets, Laptops, Desktop Computers, Cell Phones, et cetera) are locked when not in use, even if they are stepping away from these Technology Resources for a moment.

Technology Updates
End users must ensure that their Technology Resources employ the latest updates to ensure that the latest security patches are in place.

Public Setting Awareness
End users should be aware of their surroundings and ensure that sensitive UMass Global information is not exposed in a public setting where individuals can look over the user's shoulder to access such information. This extends to having conversations over the phone in public while discussing sensitive UMass Global information which could be overheard by members of the public.

Anti-Virus And Anti-Malware Protection
UMass Global provides antivirus and Malware protection on all university computers but if the end user is using a personal device it is recommended that the user have an antivirus software and anti-malware software. If such software is in place, the end user must make sure it is up to date.

Lost Or Stolen Devices
End users must immediately report lost or stolen devices so that UMass Global can remotely wipe them and to determine any risk exposure to UMass Global based on the information contained in the lost or stolen device. In certain circumstances UMass Global may engage local authorities to assist in device recovery. In addition, UMass Global may assist the end user in obtaining a replacement device and restore data from the last backup taken. Please report any lost or stolen device to the Service Desk.

Social Engineering
The increased Work From Home activity due to the Coronavirus pandemic has exposed users to increased Social Engineering susceptibility. Beware of anyone asking you for your login/password via e-mail, text, messenger, phone or other channels. If it seems suspicious, please contact the Service Desk for guidance.

Changing Work From Home Location
If the user intends to change their Work From Home location, they are required to inform UMass Global as this may have implications for Information Security as well as Coronavirus exposure and/or other health concerns.

Coronavirus

During the period of the Coronavirus Pandemic, UMass Global has implemented Work From Home policies. Anyone arriving at any UMass Global building is required to wear a mask throughout the time they are on-site, social distance if they encounter any other individual, wash their hands thoroughly before touching any furniture and Technology Resources, and log their time of entry, purpose of visit and time of exit with UMass Global. In case the user or anyone they have been in contact with has been identified as Covid-19 positive, they are required to inform UMass Global so that UMass Global may take the necessary steps to trace contacts and clean any areas, or technology resources the user may have touched in the time period they were visiting UMass Global premises.

Political Use

As a 501(c)(3) organization, UMass Global cannot participate in any political campaign on behalf of or in opposition to a candidate for public office. Similarly UMass Global may not participate in influencing legislation (i.e. lobbying). Users cannot use UMass Global Technology Resources for political purposes in a manner that suggests UMass Global itself is participating in a campaign, political activity, fundraising, or for influencing legislation.

Document last revised on Thursday, April 22, 2020.