Augusta, GA
Information Technology
Citywide Policies and Procedures

Effective June 5, 2024

Information
Technology
Augusta, Georgia

Table of Contents

1.01 Preface to Information Technology Policies & Procedures

1.01.1 PURPOSE

The Augusta Information Technology Policies and Procedures cover the use of electronic technology resources belonging to, or used by, the Augusta, Georgia government. These include, but are not limited to, all computer systems of any size and function and their attached email systems, software, network resources, Internet resources, radios, cellular telephones, and other mobile devices. All technology resources owned by Augusta are Augusta property. These systems are in place to facilitate your ability to do your job efficiently and productively. To that end, these systems are for business purposes and any personal use is prohibited.

1.01.2 OBJECTIVES

a. Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by Augusta, or any agent for Augusta.

b. Provide uninterrupted network resources to users.

c. Ensure proper usage of networked information, programs, and facilities offered by Augusta.

d. Maintain security of and access to networked data and resources on an authorized basis.

e. Secure email from unauthorized access.

f. Protect the confidentiality and integrity of files and programs from unauthorized users.

g. Inform users there is no expectation of privacy in their use of Augusta-owned hardware, software, or computer network access and usage.

h. Provide Internet and email access to users of Augusta.

i. Provide the necessary technology resources to enable employees to perform duties.

1.01.3 SCOPE

These policies shall apply to all persons, whether employees, independent contractors or agents of Augusta, or otherwise, who use Augusta's electronic technology resources. All persons using Augusta's electronic resources must comply with all software licenses, copyright laws and all other State and Federal laws governing intellectual properties.

No one shall knowingly endanger the security of any Augusta computer or network facility, nor willfully interfere with others' authorized computer usage. Many of the regulations given here deal with specific acts of this kind. You should not assume that other malicious acts or deliberate security violations are permissible merely because there is no specific rule against the action.

Approval to use Augusta's network, email systems, and Internet must first be obtained from the Department Head or authorized designee. The network, email systems, and Internet may be accessed for official business from remote PCs, including one's home personal computer.

1.01.4 OWNERSHIP AND PRIVACY EXPECTATIONS

All technology resources and all information transmitted by, received from, and stored on Augusta systems are the property of Augusta and as such, are subject to inspection by Augusta officials. Augusta has the right to monitor any and all aspects of Augusta's electronic technology resources. Augusta reserves the right to audit and monitor the information on all systems, electronic mail, and information stored on computer systems or media, without advance notice. This might include investigation of theft, unauthorized disclosure of confidential business or proprietary information, personal abuse of the system or monitoring workflow and productivity.

1.01.5 APPROPRIATE USE

At all times when an employee is using Augusta electronic technology resources, he or she is representing Augusta. Use the same good judgment in all resource use that you would use in written correspondence or in determining the "appropriate conduct": Augusta employees are expected to use all Augusta-provided electronic resources responsibly and professionally.

1.01.6 RESPONSIBILITIES

The Information Technology Department (IT) is responsible for ensuring the development, central implementation, and maintenance of these policies.

Each Augusta Department Director or Elected Official is responsible for ensuring that these policies are properly communicated, understood, and implemented within his or her respective department. Each Department Director is also responsible for defining, approving, and implementing processes and procedures within his or her department and ensuring their consistency with these policies.

All customers are responsible for complying with these policies and associated guidelines provided by their respective Department Directors. Customers are also responsible for reporting misuse of Augusta resources to Department Directors, and for cooperating with official security investigations relating to misuse.

1.01.7 STATEMENT OF CONSEQUENCES

Noncompliance with these policies may constitute a legal risk to Augusta, an organizational risk to Augusta in terms of potential harm to employees or the public, a security risk to Augusta's network operations, and/or a potential personal liability. The presence of unauthorized data in the Augusta network could lead to liability on the part of Augusta as well as the individuals responsible for obtaining it.

Any employee who discovers a violation of these policies shall notify his or her superiors through the established chain of command.

The failure of any customer to abide by these policies will result in the denial, revocation, or suspension of computer network and Internet privileges. Furthermore, any employee who violates the terms of these policies may be subject to disciplinary action up to and including termination of employment.

1.01.8 DISCLAIMER

Due to rapid changes in technology, these policies and procedures are subject to change without notice at any time. All changes will be posted in a timely manner for all employees to review.

1.02 Definitions

1.02.1 PURPOSE

Throughout these policies, except where the context clearly indicates otherwise, the following words and phrases shall have the meaning indicated below.

Due to the rapid pace of technology changes, specific terminology may become obsolete quickly. Customers should assume that these policies apply to all technology platforms used by this organization and its employees, even if a particular technology is not specifically named.

1.02.2 DEFINITIONS

- Augusta – the Augusta, Georgia Government.
- Augusta computers and network facilities – all computers owned and administered by Augusta or connected to Augusta's communication facilities, including departmental computers, and Augusta's computer network facilities accessed by anyone from anywhere.
- Authorization – permission granted by the Administrator of Augusta and/or the Chief Information Officer within Augusta government.
- Customer/User – as used in this policy, refers to all Augusta employees, elected and appointed officials, independent contractors and other persons or entities accessing or using any of Augusta's electronic technology resources.
- Department Director – head of an Augusta department or agency, including appointed directors and elected officials.
- Download – to receive a file transmitted over a network.
- Email – the ability to compose and distribute messages, documents, files, software, or images by electronic means over a phone line or network connection. This includes internal and external email.
- Employee Portal – an internal computer network that offers Internet-like functions, allowing departments to maintain and access information that is not part of a public Internet presence.
- Intellectual Property – rights and products of the mind or intellect, arising under any law, including, but not limited to Trade Secrets, Trademarks, Trade Dress, Copyrights, and Unfair Competition.
- Internet Service Provider (ISP) – an entity that charges startup and monthly fees to users and provides them with the initial host connection to the rest of the Internet.
- Malicious Emails – any email communication used to damage or attack a computer, user, system or network. Malicious emails often attempt to trick users into downloading malware or into revealing confidential information, like passwords or credit card information. Phishing emails are one common type of malicious email.

- Malware – any malicious software intentionally designed to damage or attack a computer, user, system or network. Malware can include viruses, spyware, ransomware, Trojan Horses, and many other categories of harmful software. Anti-virus software is designed to help defend computers against malware.
- Mobile Device – any portable computing or communication device, such as a cellular phone, smartphone or tablet.
- Network Resources – the hardware and software necessary to connect computers and resources into a communication system.
- Public Record – a record that is made by a public official in the pursuance of a duty to disseminate information to the public or to serve as a memorial of official transactions for public reference.
- Social Media Sites and Services - online technologies and practices that people use to share opinions, information, and requests. Social media can take many different forms, including text, images, audio, and video. A few prominent examples of social media platforms are Facebook, Twitter, Instagram and YouTube.
- Upload – to transmit/send a file over a network.

1.03 Computer Acceptable Use

1.03.1 PURPOSE

The purpose of this policy is to establish guidelines and requirements governing the requisition and acceptable use of Augusta-provided computers. Adherence to this policy will minimize risks to Augusta while providing a productive tool.

The Augusta computer acceptable use policy (hereafter referred to as "Computer Policy") applies to all computers and components (hardware and software) utilized by Augusta customers. All persons using Augusta computers must read and review this policy.

1.03.2 ACCEPTANCE OF POLICY

Use of Augusta's computers constitutes acceptance of this policy.

Augusta's computer resources are provided on an as-is, as-available basis. Augusta makes no warranties of any kind, either expressed or implied, in connection with its provision of access to and use of said resources. Augusta shall not be responsible for any claims, losses, damages, or costs of any kind (including attorney's fees) suffered, directly or indirectly, by any customer arising out of the customer's violation of this policy. Each customer is responsible for the customer's own use. No one using Augusta's computers is permitted to incur costs or liabilities during such use without prior express written authorization from the Chief Information Officer and the customer's Department Director/Manager. No financial responsibility will be assumed by Augusta for any costs or liabilities or damages caused to anyone as a result of a customer's violation of this policy.

1.03.3 ACCESS

Augusta's computers are the property of Augusta. Augusta's computers are intended for the lawful and appropriate conduct of Augusta business and are reserved for that purpose. All customers using Augusta's computers are expected to act and to communicate professionally, using them in furtherance of Augusta business.

Each customer is responsible for the content of all electronic data that the customer creates, stores, and uses. No customer has personal privacy rights in any document, email, or email attachment created, received, or sent using Augusta's computers.

Employees, officials, contractors, interns, and other individuals may be granted access to Augusta's computers for the conduct of Augusta business. Department Directors retain the discretion at all times to deny access to any employee, however.

1.03.4 AUTHORIZED ACCESS

Only computers purchased, leased, or rented by Augusta may be used for conducting Augusta business. Only employees of the Information Technology Department are authorized to install and provide access to computers.

All unauthorized installations are subject to removal.

No employee shall:

1. Use Augusta's computers to commit wiretapping; unlawful interception of electronic communications; infringement of copyrights trademarks, other proprietary rights, or license agreements; computer crimes; or any other violation of local, state or federal laws or regulations.
2. Gain unauthorized access to information that is confidential or protected or attempt to do so.
3. Run programs that attempt to identify passwords or codes.
4. Read, copy, change, or delete another person's work without that person's express permission.
5. Use another person's password or allow others to use theirs.
6. Use assumed names.
7. Attempt to evade, disable, encrypt or mask, use someone else's identity and/or password or otherwise bypass existing access restrictions or other security provisions of the computer network.
8. Knowingly disclose attorney-client communications or attorney work products.
9. Disclose data known to be confidential or which should be known to be confidential.
10. Use Augusta's computers for personal gain.
11. Use Augusta's computers for solicitation of non-Augusta business, gambling, or entering contests or sweepstakes.
12. Attempt to connect to any other Augusta computer without authorization of the Information Technology Department.
13. Use Augusta's computers to conduct internal union business or any other non-Augusta business.
14. Install or distribute any non-Augusta business-related software and data including, but not limited to, animations, screen savers, wallpaper, etc. without the express prior approval of the Information Technology Department.

1.03.5 ELECTRONIC DATA RECORDS AND FREEDOM OF INFORMATION

Documents produced and stored using Augusta's computers in the conduct of Augusta business are "public records" and subject to disclosure under the Georgia Open Records Act and the Federal Freedom of Information Act (FOIA), unless an exemption to disclosure applies.

Reasonable caution should be exercised with respect to the creation, storage, and usage of all data, private and public, stored on Augusta's computers, as all such data are potentially public records subject to disclosure. Where statutes or regulations govern the storage or archiving of particular data, this policy requires that such statutes and regulations must be followed. The Augusta Law Department is responsible for determining which records are subject to disclosure under Georgia and Federal law.

1.03.6 MONITORING

You are hereby notified that when Augusta has reasonable grounds to believe that an employee is engaged in conduct which (i) violates the law, (ii) violates the legal rights of Augusta or violates the legal rights of Augusta employees, (iii) creates a hostile workplace environment, or (iv) violates government and/or employee policy, and electronic monitoring may produce evidence of this misconduct, Augusta may conduct electronic monitoring of the employee in question without prior written notice.

To initiate electronic monitoring, an Augusta Department Director or Elected Official must submit a written request through the Augusta Law Department. Information Technology will conduct the monitoring process as requested. Information Technology will then release the collected information to the Augusta Law Department, which will determine which information is subject to disclosure to the requestor.

Any other individual or agency seeking technology-related records must follow the Open Records Request process managed by the Administrator's Office.

“Electronic monitoring” means the collection of information on Augusta’s premises concerning a Augusta employee’s activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photo-electronic or photo-optical systems, but not including the collection of information for security purposes in common areas of Augusta premises which are held out for use by the public, or collection of information prohibited under state or federal law.

1.03.7 MISREPRESENTATION

No one shall misrepresent his or her identity or relationship to Augusta when obtaining or using Augusta computer or network privileges. On some systems, there are ways to post messages without revealing your name and address. Anonymous communication is permissible when there is a legitimate need for additional privacy. It is not a cover for fraudulent or obnoxious behavior, and in cases of abuse, anonymous messages can be traced to their source. Deceptive communication, in which you claim to be some other specific person, is never permitted.

You must not claim to be someone else, nor claim to have a different relationship to Augusta than you actually do, when obtaining a computer account or access to a lab. You must not falsify your name, address, email address, or affiliation when sending email or other messages from a Augusta computer. Doing so can be illegal (Ga. Code 16-9-93.1 and other laws against misrepresentation) as well as being an unacceptable use of Augusta's facilities.

1.03.8 ENFORCEMENT

The Information Technology Department has access to all data stored on Augusta's computers and is authorized as necessary to monitor compliance with this policy and to conduct any electronic monitoring. The Chief Information Officer will review alleged violations of this policy in the use of Augusta's computers on a case-by-case basis. Clear violations of this policy may result in termination of access to the computer for the person(s) at fault.

In addition, the Chief Information Officer shall refer all violations of this policy for possible disciplinary action to the appropriate supervisory authority. All supervisory authorities are required to enforce this policy and are authorized to issue appropriate discipline including possible discharge from employment for violations of this policy. Violations of law in the use of Augusta's computer network subject to possible criminal sanctions will be referred to the appropriate Richmond County, State of Georgia, and/or Federal agency.

1.04 Network Resources and Internet Acceptable Use

1.04.1 PURPOSE

Many Augusta employees have been provided with access to network resources so that they may conduct official Augusta business. Augusta reserves the right, without prior notice, to monitor this use. This policy outlines specific guidelines which apply to the use of network resources. <u>Based on their unique needs, Department Directors may adopt additional provisions and/or more restrictive policies that do not conflict with this policy.</u>

1.04.2 ACCEPTABLE USE AND MONITORING

Internet access is provided to Augusta employees for conducting official Augusta business to reduce costs or as a means to provide more accurate and complete information to Augusta constituents. Once an outbound connection is established, all Internet access activity is electronically monitored on a continuous basis. Note: All references to "Internet" in this policy apply to the Employee Portal as well.

Augusta employees, vendors/business partners and other governmental agencies may be authorized to access Augusta's network resources to perform business functions with or on behalf of Augusta. Anyone using the network must be acting within the scope of their employment or contractual relationship with Augusta and must agree to abide by the terms of this agreement as evidenced by his or her signature on the respective forms.

1.04.3 USE OF SHARED RESOURCES

All customers shall share computing resources in accordance with policies set for the systems involved, giving priority to more important work, and cooperating fully with the other customers of the same equipment. The administrators in charge of the system, in consultation with the customer community, set priorities for any particular machine or platform.

If you need an unusual amount of disk space, bandwidth, or other resources, check with the administrator(s) in charge of the system rather than risk disrupting others' work. When resources are limited, work that is necessary to Augusta's mission must take priority over computing that is done to pursue personal interests or self-training on side topics. In addition, no matter how important your work may be, you are only entitled to one person's fair share of these resources unless additional resources are available and appropriate permission has been granted.

Obtaining extra computer resources through any form of deception (e.g., secretly opening multiple accounts, misrepresenting the nature of your work, or the like) is strictly prohibited.

1.04.4 SECURITY ACCESS

Augusta's firewall restricts access to certain websites from the Augusta network. In addition, only Information Technology personnel can download executable files from the Internet. These restrictions protect the network from malware and other unauthorized software. If you are being blocked by the firewall in trying to access a work-related website or download, send an email to the IT Help Desk with the website URL and where in the website you received the firewall message. If the website is approved as a legitimate work-related website, it will be added to the exception list to allow customer access. Unrestricted access to the Internet by anyone, employee or vendor, will not be allowed for any reason.

1.04.5 STATEMENT OF CONSEQUENCES FOR MALICIOUS USE

State and federal laws forbid malicious disruption of computers. Augusta does not tolerate individuals who invade others' privacy, steal computer services, or commit misrepresentation or fraud, nor pranksters who attempt to disrupt computers or network facilities for any other purpose.

Individual employees are responsible for their conduct as Internet customers. Augusta shall assume no liability or responsibility for, and shall not defend or indemnify an employee against, any charges resulting from any action that is found to be in violation of this policy. The Information Technology Department advises employees that no legitimate expectation of privacy can be asserted in their use of Augusta’s computer systems including, but not limited to, their use of the Internet whether the use is part of the employee’s personal use or Augusta-related use. The Information Technology Department reserves the right to review employee’s computer files and/or monitor their Internet usage at any time to maintain system security and integrity, or to determine possible violations of policy or law.

Using a computer without permission is theft of services and is illegal under state and federal laws. In addition, state law (GA Code 16-9-90 et seq.) defines the following specific computer crimes:

- Computer theft (including theft of computer services, intellectual property such as copyrighted material, and any other property)
- Computer trespass (unauthorized use of computers to delete or alter data or interfere with others' usage)
- Computer invasion of privacy (unauthorized access to financial or personal data or the like)
- Computer forgery (forgery as defined by other laws, but committed on a computer rather than on paper)
- Computer password disclosure (unauthorized disclosure of a password resulting in damages exceeding $500)
- Misleading transmittal of names or trademarks (falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal)

Maximum penalties for the first four crimes in the list are a $50,000 fine and 15 years of imprisonment, plus civil liability. The maximum penalties for computer password disclosure are a $5,000 fine and 1 year of imprisonment, plus civil liability.

1.04.6 PROHIBITIONS

Employees are expressly forbidden to misuse any network resources or Internet or Employee Portal access privileges in ways that may include, but are not limited to:

1. Using the Internet or network resources in support of unlawful activities as defined by federal, state, and local law. (Note: Employees or other customers using the email/Internet systems in violation of local, state, national or international laws may be prosecuted.)

2. Uses that violate existing Augusta policies, including policies on sexual harassment, discrimination and harassment, or workplace violence. This prohibition would include viewing, transmitting, or downloading material that is sexually explicit, that creates a hostile work environment, or that promotes hatred or violence. This prohibition does not apply to Augusta employees in Public Safety for whom this activity is part of carrying out their assigned duties.
3. Making threats against other persons or institutions.
4. Sending or sharing with unauthorized persons any information that is confidential by law, rule, or regulation.
5. Deliberately viewing, downloading or uploading material containing the following that is not in support of business functions:
    a. Derogatory racial content.
    b. Derogatory religious content.
    c. Slanderous language and/or comments.
    d. Sexual content.
    e. Political statements.
    f. Offensive language, language of a harassing nature or graphical gestures.
    g. Materials that reflect negatively on Augusta Government.
    h. MP3 (music) files or AVI, MPEG, etc. (audio/video/movie) files.
    i. Non-job-related Internet streaming media content, such as Internet radio broadcasts or streaming video.
    j. Any software/program that compromises computer security or may introduce malware into Augusta systems.
    k. Any non-standard or non-business-related files or software unless previously approved by Information Technology.

6. Downloading, copying, installing, or using any software or data files in violation of applicable copyrights or license agreements and not authorized by Information Technology and not approved by Augusta.

    a. This rule forbids making unauthorized copies, for use elsewhere, of software residing on Augusta's computers. It also forbids installing or using pirated software on Augusta computers. Only Augusta-authorized software shall be installed or used on Augusta-owned or leased hardware. The use of unlicensed software copies (software used in violation of the software license), personally owned software, and unauthorized software is strictly forbidden. Information Technology or IT-authorized personnel only should only perform these software installations. The price of a piece of software is not just the cost of the disk - it's also one customer's share of the cost of developing and supporting it. It is wrong to use software without paying your fair share. Unauthorized copying is a violation of federal copyright law.

    b. *License checks:* If strangers show up at your computer site saying they are there to check software licenses, you should immediately contact Information Technology and your administrative superiors. Software licenses do not normally authorize these surprise inspections, and there is a substantial risk that the "inspectors" are not legitimate.

7. Connecting a computer/device to any portion of Augusta’s networks unless it meets the technical and security standards set and authorized by Information Technology. (For specific information, contact Information Technology.)

8. Improperly accessing, reading, copying, misappropriating, altering, misusing, or destroying the information/files of other customers.

9. Attempting to gain access to computers or networks to which they do not have legitimate access, or violating the acceptable use policies of any network to which they connect, or mounting any attack on the security of any system. Absolutely no infiltration of another's network or other parts of their electronic communications systems is allowed (i.e. hacking, cracking). Persons conducting such activity are subject to prosecution by law.

10. Misrepresentation as someone else, real or fictional, or sending messages anonymously.

11. Modifying or reconfiguring the hardware, operating system, or application software of an Augusta computer unless someone from Information Technology has given permission to do so. The other customers with whom you share the machine, and the technicians on whom you rely for support, are expecting to find it set up exactly the way it was configured.

    a. Only IT personnel or IT authorized personnel should move computers, printers, monitors, or other technology devices.

    b. Relocation of computer and computer-related peripherals are handled by placing a request with the department’s IT Project Manager.

c. Any cost incurred by a customer attempting to repair and/or relocate equipment will be borne by the employee responsible.

12. Leaving workstation unattended without engaging password protection for the keyboard or workstation.

13. Unauthorized connection of multiple computers for sharing resources.

14. Accessing or attempting to obtain access to any Augusta computer or network facility for non-Augusta business. By law, Augusta can only provide computer services for its own work, not for private use. In this respect, Augusta's computers are different from those owned by colleges or corporations.

15. Accessing or attempting to obtain access to any Augusta computer or network facility for political campaigns, fundraising, commercial enterprises, mass mailings, or other outside activities that have not been granted the use of Augusta's facilities. Furthermore, you should be aware that the ability to use a computer and/or service does not constitute permission or authorization. If you have questions, contact your supervisor or Information Technology.

16. Creating a public display of Augusta information on the Internet, such as departmental websites, without prior notification to the Information Technology Department to ensure content and web navigation.

1.05 Email and Internet Communications

1.05.1 PURPOSE

Many Augusta employees have been provided with email and Internet access so that they may conduct official Augusta business. Customers must take full responsibility for messages that they transmit through Augusta’s computers and network facilities. Augusta reserves the right, without prior notice, to monitor email and Internet use. This policy outlines specific guidelines that apply to the use of email and Internet communication resources, including guidelines for acceptable and unacceptable communications.

1.05.2 ACCEPTABLE USES

In compliance with applicable laws, employees of Augusta should use email to further Augusta’s mission and to provide service of the highest quality. Job-related email will be sent and received through Augusta's email facility.

Email and Internet access should be used for “appropriate business use" only—that is, for the employee's job-related duties and responsibilities. This policy recognizes the specific definition of appropriate business use may differ among departments based on their mission and functions. Therefore, each department should define appropriate business use and ensure employees are informed of their guidelines.

No one shall use Augusta's computers to transmit fraudulent, defamatory, harassing, obscene, or threatening messages, spam, or any communications prohibited by law. Customers have exactly the same responsibilities on the computer network as when using other forms of communication.

1.05.3 PROFESSIONALISM

Employees have an obligation to use their access to the Internet and email in a responsible and informed way, conforming to network etiquette, customs, courtesies, and any or all applicable laws or regulations, including copyright restrictions.

Employees must be aware that their conduct or information they publish could reflect on the reputation of Augusta. Therefore, professionalism in all communications is of the utmost importance. Employees shall represent themselves and Augusta accurately and honestly through electronic information or service content. Departments are responsible for the content of their published information and for the actions of their employees.

Employee emails should include official departmental signature blocks, including relevant contact information. Quotes, cartoons, and other personal content are inappropriate for professional communication and are not allowed in email signatures.

Use prudent caution when sending out any message that appears to be an official communication from Augusta. If the header identifies your message as coming from an administrative office or from the office of someone other than yourself (e.g., “Clerk of Court”), recipients will presume that you are speaking for that office or person.

Bear in mind that uninvited amorous or sexual messages are likely to be construed as harassment. If you are bothered by uninvited email, ask the sender to stop, and then, if necessary, consult Human Resources.

1.05.4 MALICIOUS EMAILS

Malicious emails are a common way that cybercriminals target employees and the Augusta organization. These emails often attempt to trick users into downloading malware or into revealing confidential information, like passwords or credit card information. Be very cautious in opening email attachments and in clicking links in emails, particularly for emails from outside the Augusta network. Never send sensitive personal information through email. If you have concerns about a suspicious email, contact the Information Technology Help Desk.

1.05.5 TRANSMISSION OF CONFIDENTIAL INFORMATION

Departments who choose to use email to transmit highly sensitive or confidential information should be aware of the potential risks of sending unsecured transmissions. At a minimum, emails of this nature should contain a confidentiality statement. Employees may also send encrypted emails by adding the tag [SECURE] to the beginning of the subject line.

1.05.6 GENERAL EMPLOYEE SEPARATION

When an employee separates from employment with Augusta, Information Technology receives an official separation notice from Human Resources. Information Technology will terminate the employee’s email and network access on the effective date set by Human Resources.

If circumstances require immediate suspension of the employee’s access, the Department Director, Human Resources Director, or Administrator’s Office may make this request to the Chief Information Officer or designee.

Upon an employee’s separation or reassignment to another Augusta department, the Department Director will assess the need to retain the employee’s previous emails. If retention is required, the Department Director must send a written request to the Chief Information Officer or designee. (The request must be made prior to Information Technology receiving written notice of termination from Human Resources.) Information Technology will provide the requesting department with access to the employee’s email, as long as the files are still available. All files will then be deleted from the system. **If a request is not made, all files will be removed upon Information Technology receiving notice of termination from Human Resources.**

If an employee transfers from one department to another and requests their previous email be restored, Information Technology will require written authorization (email or memo) from all previous departments for which the employee has worked. This authorization should accompany the request in the Information Technology work order system.

1.05.7 ELECTED OFFICIAL SEPARATION

When an elected official leaves office, Information Technology will terminate his or her email and network access on the day after the official's last day in office. For most officials, this date would be January 1.

Information Technology will provide written notice in December each year to all outgoing elected officials regarding their upcoming access termination. This notice will also be copied to the Administrator, Clerk of Commission, and Court Administrator (as needed).

When access is terminated, the account will be deleted, but the account's data file (.pst file) will be retained for future open records requests.

When elected officials leave or are removed from office during their term, the same policy will apply. Information Technology will terminate these officials' email and network access immediately upon their departure from office.

In all cases, the elected official's office/department will be responsible for verifying that access has been terminated appropriately.

1.05.8 PUBLIC RECORDS AND EMAIL RETENTION

Email created, sent, or received in conjunction with the transaction of official business are public records in accordance with Georgia's Freedom of Information Act (FOIA) and Public Records Act (PRA). A public record is defined as follows:

> "all books, papers, maps, photographs, cards, tapes, recordings, or other documentary regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body."

As such, each individual has the responsibility to retain their own business-related email and manage it according to the retention schedules established for paper records. Emails of a non-business nature are discouraged and should be deleted immediately.

Retention of electronic transmittals shall be addressed in each department's retention policy. Each department shall establish the retention criteria for essential electronic mail and other electronic records within their own department and not rely on Information Technology.

Customers shall retain all electronic messages when aware of an Open Record Request or when there exists a reasonable anticipation and/or likelihood of litigation.

The Augusta Law Department will determine which records are subject to disclosure under Georgia Law.

1.05.9 MONITORING AND EXPECTATIONS OF PRIVACY

This policy applies when Augusta resources are being used by employees, regardless of the time of day, location, or method of access. Monitoring tools are in place to monitor employees' use of electronic mail and the Internet. Employees shall have no expectation of privacy associated with email transmissions and the information they publish/store on the Internet using Augusta's resources. Employees shall cooperate with any investigation regarding the use of their computer or their activities associated with Information Technology resources.

1.05.10 AUTHORIZATION AND INSTALLATION BY INFORMATION TECHNOLOGY

Internet access, hardware, and software must be authorized and installed by Augusta Information Technology personnel or Information Technology-approved personnel.

1.05.11 OTHER EMAIL SERVICES

Customers should not use electronic mail services other than those maintained by Augusta Information Technology while on the secured Augusta network. Personal accounts should never be used to conduct Augusta business. These services present security concerns and use much more bandwidth than local mail servers, which can negatively impact network performance.

1.05.12 MASS EMAIL NOTIFICATIONS

All organization-wide email notifications must be business-related and submitted to the Administrator's Office by way of the following email address for review and distribution: Employee_Communications@augustaga.gov. The only exceptions to this policy are urgent or emergency communications from Information Technology or the Emergency Management Agency, which may be sent directly by those departments through Augusta Notice.

See 1.16 Augusta Mass Email Guidelines for more information and guidance on the content of organization-wide email notifications.

1.05.13 EMAIL GROUPS

Requests by Department Directors for new email groups or changes to an existing email group should be made in writing. Normal practice is to restrict access to the group to only the requesting Director unless additional customers are requested in writing by said Director. This policy pertains to all organization-wide email groups as well as internal department email groups.

For example, a new email group is requested for all Nationwide Retirement participants. Since this is an employee benefit, written documentation should be received from the Director of Human Resources regarding who to include in the group as well as who has access to email this group. If no additional names are submitted with the request, only the Director of Human Resources would have access to email this group.

1.05.14 COMMERCIAL USE OF INTERNET COMMUNICATIONS

The Augusta Commission must approve any commercial use of Internet communications by departments. Departments shall not accept commercial banner ads or vendor-hosted website advertising for which the department receives compensation. As a general practice, Augusta avoids endorsing or promoting a specific product or company from our websites or through email.

1.05.15 PERSONAL SOCIAL MEDIA ACCOUNTS

Employees have the First Amendment right to free speech and are thus not restricted in general in using personal social media sites in their personal lives. It is recommended that these sites remain personal in nature to help ensure a distinction between sharing personal and organizational views. Employees should keep their privacy and security in mind when engaging in personal social media use. Even with good security measures, the comments made (and how those comments may be interpreted) could be forwarded and accessible to others for a long time.

Public safety and sworn officials should reference their respective departmental policies regarding acceptable use of social media.

Personal social media accounts should not be accessed from the Augusta secured network or used to conduct Augusta business. Employees should not use Augusta email accounts or passwords in conjunction with personal social networking accounts. (Employees who are responsible for maintaining official Augusta social media accounts are exempted from these restrictions.)

Employees should be aware that threatening, abusive, or harassing communications with other employees through personal social media accounts is subject to the same investigation and disciplinary action as other forms of communication.

Employees may list their Augusta position in their personal social media accounts, but they are not authorized to speak or comment on behalf of Augusta. If an employee is contacted by a resident or elected official on their personal social media account regarding Augusta business, employees are encouraged to redirect the resident or official to an official Augusta communications channel.

If an employee chooses to post photos/live tweet/live stream information about an internal Augusta meeting, staff training, or employee-only event or activity, the employee must notify the meeting organizer as well as others in attendance of the intention to post and receive permission from all involved. The requesting employee must refrain from posting content depicting or quoting anyone at an Augusta-related event who withheld permission.

1.05.16 PROHIBITIONS

While using Augusta-provided Internet access and email, employees are strictly prohibited from the following:

1. Transmitting any communications that may constitute or that contain any of the following:

a. Verbal abuse, threats, intimidation, slander, expletives, sexual harassment, or harassment of any kind.

b. Statements, language, images or other materials that are reasonably likely to be perceived as offensive or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.

c. Abusive or objectionable language in either public or private messages.

d. Sexually oriented messages or images, including disseminating, soliciting or storing this content.

e. Solicitations for money for religious or political causes, or advocating religious or political opinions.

f. Proprietary or confidential Augusta or personal information when directed to any unauthorized recipient, or sending confidential email without the proper security standards (including encryption if necessary) being met. This includes any information that constitutes an unwarranted invasion of personal privacy.

g. Copyrighted materials (including articles, images, games, or other software) in violation of copyright laws.

2. Reposting, forwarding or performing group broadcasts (including chain letters) of any messages without prior consent of management.

3. Posting information or opinions of confidential Augusta matters on message boards, in chat rooms, in news groups, on social media, or other public platforms.

4. Using the Internet and email for personal gain or personal business activities, such as buying or selling of good or services with a profit motive.

5. Developing or maintaining a personal web page on or from an Augusta device.

6. Creating, installing, or knowingly distributing any material that contains malware on any Augusta computer or network facility, regardless of whether any demonstrable harm results.

   i. Even when the harm done by programs of these types is not readily evident, they confuse beginning computer customers, degrade CPU performance, and waste the time of system administrators who must remove them.

   ii. It is the responsibility of the customer to provide malware/anti-virus protection on any files loaded, transmitted, or downloaded in any way to an Augusta computer. This includes the latest available updates.

7. Misrepresenting, obscuring, suppressing, or replacing a customer’s identity on the Internet or email. This includes the use of false or misleading subject headers and presentation of information in the distribution of email as well as sending messages anonymously.

1.06 Usernames and Passwords

1.06.1 PURPOSE

Passwords are an important aspect of computer security. They are the front line of protection for customer accounts. A poorly chosen password may result in the compromise of Augusta's entire network. As such, all Augusta employees (including contractors and vendors with access to Augusta systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This policy summarizes Augusta's username and password policies and procedures. The intent of this policy is to provide a safe computing environment on the Augusta Information Technology network and maintain the integrity of security on these systems.

1.06.2 USERNAME ASSIGNMENT

Employee network accounts will be created when an authorized representative from the customer department submits a security request via the online Security Request Portal. The request must contain the new employee's full name, employee ID, title, phone number, supervisor, and suggested email address (auto-created by form).

Customer IDs (usernames) will be created based on employee names in the enterprise financial system. Aliases, nicknames, etc., will not be permitted. The general naming convention is to include the employee's first initial and last name (e.g., TWilliams). If following this convention would create a duplicate--for example, Troy Williams and Teresa Williams--the employee's middle initial will be used (e.g. TAWilliams). In instances when two employees have the same first and middle initial and last name, numbers will be added following the employee's name (e.g., TAWilliams2). Generic username accounts are not permitted.

1.06.3 PASSWORDS

Passwords are the entry point to our IT resources and are an essential part of ensuring that our systems remain secure. Passwords protect Augusta's entire network, not just the individual machines to which they apply. Augusta insists that each account be used only by the person to whom it belongs, so that if problems are detected or abuse is alleged, the responsible person can be identified. If a department cannot keep passwords secure, it cannot connect its machines to the Augusta-wide network.

No one shall give any password for any Augusta computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one except the System or Network Administrator in charge of a computer is authorized to issue passwords for that computer. If legitimate access is required, the proper request must be made to Information Technology in writing from the Department Director. Computers and networks are just like any other Augusta facilities and are to be used only be people who have permission.

1.06.4 PASSWORD HANDLING

Passwords for *all* systems are subject to the following rules:

1. Every customer account on each machine shall have only one person authorized to use it. Every customer will be allowed to login to only one machine at a time. If a customer needs the ability to login to more than one machine at a time to do their job, they may make a request through their Project Manager to have multiple logins granted. That customer will be required to authenticate their identity to the system using some proof of identity such as by password or passphrase.
2. **Never share your password with anyone else.** Likewise, you must never use or disclose a password that was given to you improperly.
    a. No passwords are to be shared in order to "cover" for someone out of the office. Contact Information Technology to create a temporary account if there are resources management needs to access. This request must come in writing from the Director/Elected Official.

    b. No passwords are to be spoken, written, emailed, hinted at, shared, or in any way known to anyone other than the customer involved. This includes supervisors and personal assistants.

    c. All passwords are to be treated as sensitive, confidential Augusta information. If someone demands a password, refer him or her to this document or have him or her call the IT Help Desk.

    d. **Information Technology will never ask for your password.**
3. Passwords are not to be displayed or concealed in your workspace. Do not store the password for one computer in another computer unless your system administrator has assured you that no security hazard will result. It is easy for a stranger to walk up to your personal computer and retrieve passwords that are stored in it.
4. Do not use the same password for Augusta accounts as for other non-Augusta access (e.g., personal email account, benefits accounts, accounts on other websites, etc.)
5. Do not use the “Remember Password” feature of web browsers or applications.
6. Your password is secret. Information Technology staff will not normally ask you for it. The computer will never ask you to type it unless you are logging in or changing your password. Beware of computer programs that ask you to "log in again" or type your password at any other time; they are likely to be tricks. (There are rare exceptions on some computers; check with the IT Help Desk. If anything that you do not understand ever happens after you type your password, then change your password immediately.)
7. Failed login attempts will be logged. More than three failed logins on a given account per hour will require investigation.
8. If you feel a password is compromised, the password should be changed immediately. Please call the Information Technology Help Desk at (706) 821-2524 for assistance if necessary.

1.06.5 PASSWORD COMPOSITION

You are responsible for choosing a secure password. Do not use your name, address, date of birth, username, nickname, telephone numbers or any term someone who is familiar with you could easily guess. Avoid recognizable words in any language, because some people guess passwords by automatically trying every word in a large dictionary. A good way to make up a secure password is to use the initials of a phrase and include some numbers or special characters as well as upper and lowercase letters. For example, *57ityDwb!! is a good password, and it's easy to remember because it stands for "57 is the year Dexter was born!!"

Augusta's network and client operating systems have systematically enforced password requirements. Passwords must meet the following criteria:

- Password may not contain all or part of the customer's account name.
- Password is at least twelve characters long.
- Password contains characters from all four of the following categories:
  - English uppercase characters (A…Z)
  - English lowercase characters (a…z)
  - Base 10 digits (0…9)
  - Non-alphanumeric special characters (exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], etc.)

Poor, weak passwords have the following characteristics:

- The password contains less than twelve characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+
- Are at least twelve alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

1.06.6 STATEMENT OF CONSEQUENCES

Giving your password to an unauthorized person can be a crime under Georgia law. The criterion for disclosure is not whether you trust the person, but whether Augusta has authorized them.

Computer password disclosure is defined as the unauthorized disclosure of a password resulting in damages exceeding $500. In practice, this includes any disclosure that requires a system security audit afterward.

Misleading transmittal of names or trademarks is defined as falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal (GA Code 16-9-93.1).

Maximum penalties for these offenses may be up to a $50,000 fine and 15 years' imprisonment, plus civil liability. The maximum liability for computer password disclosure is a $5,000 fine and 1 year of imprisonment, plus civil liability.

1.07 Virtual Private Network Access

1.07.1 PURPOSE

This policy outlines Augusta's guidelines and requirements for employee access to the Augusta network through Virtual Private Network connections.

1.07.2 DEFINITION

A Virtual Private Network (VPN) provides a secure (encrypted) network connection over the Internet between an individual and a private network. By using the public Internet for data transport, VPN provides a low cost solution to remote access or connectivity. In effect, this allows Augusta employees to access Augusta network resources as if they were on campus.

The VPN connection is established by running special software on the remote computer that communicates with specific hardware located in Augusta's data center. The VPN hardware is assigned a unique Internet address, which is programmed into the remote software. Access is granted to users by login, using an account name and password combination.

1.07.3 GENERAL VPN POLICIES

Augusta employees, Department Directors, Administrators and Elected Officials are permitted access through a VPN with the approval of the requestor's supervisor and/or the Chief Information Officer. VPN is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally:

1. VPN access is provided through Information Technology. No other department may implement VPN services.
2. Only the VPN software distributed by Information Technology may be used on Augusta-owned devices.
3. The VPN software can only be installed on the computer listed on the VPN Access Request Form.
4. VPN access will be controlled using an account name and password. These will be assigned by the IT Security Administrator or authorized delegate.
5. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to the Augusta network.
6. When actively connected to the Augusta network, all traffic to and from the remotely attached PC is through the VPN tunnel, including Internet browsing.

7. All network activity during a VPN session is subject to Augusta policies and may be monitored for compliance.
8. All computers connected to the Augusta network via VPN or any other technology must use the most up-to-date anti-virus software that meets or exceeds the corporate standard. All computers are also required to be up to date on all OS patches for security. Proof of compliance is required prior to the assignment of a VPN account to ensure network health.
9. Compliance of anti-virus software and OS patches will be validated every time you connect to the Augusta network via the VPN. Any device that is not compliant will be quarantined and not allowed to connect until the anti-virus and/or OS has been updated to the current level.
10. VPN users will be automatically disconnected from the Augusta network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
11. The VPN concentrator is limited to an absolute connection time of 6 hours.
12. Users of computers that are not Augusta-owned equipment must configure the equipment to comply with Augusta's VPN and Network policies.
13. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Augusta network, and as such are subject to the same rules and regulations that apply to Augusta-owned equipment, i.e., their machines must be configured to comply with all Augusta network access policies.

1.07.4 SUPPORT

Due to the tremendous variation in home PC and network configurations, Information Technology is unable to provide full and immediate support for VPN-related problems. Account-related issues may be resolved by the Help Desk. For VPN networking and application issues, you may open a ticket at the Help Desk which will be addressed during regular work hours. Users will be responsible for supporting their personal computer as well as any Internet connectivity issues.

Disclaimer: Use of a router is available for any broadband plan. Hypothetically, you could have an unlimited number of computers on the Internet at one time, depending on the limitations of your router. Augusta does not endorse any particular product. Augusta does not support LANS/Networks other than our own. Augusta does not offer educational/technical support for third party equipment. For further assistance regarding your router or other equipment, you should contact the Router/LAN device manufacturer or the company that sold you the equipment.

1.07.5 OBTAINING VPN ACCESS

The following procedures should be followed to acquire VPN access:

1. Discuss the viability of remote access with your immediate supervisor.
2. If the supervisor approves, submit a request for VPN access using the VPN Employee Access Request form at https://augustaga.sharepoint.com/sites/portal.
3. Once the form has been approved by the Department Director or designee and the IT Security Administrator, you will be allowed VPN access.
4. The IT Help Desk can assist with installation of the Cisco AnyConnect VPN client.

1.07.6 CONNECTIVITY REQUIREMENTS

VPN connectivity requires an Internet Service Provider that allows VPN connections through their service. Broadband service is required (cable or DSL). Dial-up modems are not supported.

Up-to-date operating systems are required for connectivity. The current hardware/software requirements for connectivity are listed below. This list is subject to change with advancements in technology.

- **Windows** 10, 8.1, 8, and 7
- **Mac** OS X 10.8 and later
- **Apple App Store:** for Apple iOS 6.0 and later
- **Google Play**: for Android 4.0 and later

  Note that there are multiple AnyConnect images available, so it is important that you select the correct image for your device. See the Android release notes for specific requirements.
- **Windows Store**: for Windows Phone 8.1 Update 1 and later
- **BlackBerry App World**: for BlackBerry 10.3.2 and later
- **Google Chrome OS**: for Chrome OS 43 and later (early preview)
- **Amazon Appstore**: for select Kindle and Fire Phone devices

1.07.7 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action.

1.08 Workstation and Data Access

1.08.1 PURPOSE

Access to employee workstations must be restricted to the individual to whom the equipment is assigned. This policy outlines the general guidelines for managing access to employee workstations and data.

1.08.2 MAINTAINING EMPLOYEE WORKSTATIONS

As a general rule, customers should keep food and beverages away from the area around their computers and equipment to prevent accidental spills and damage. Customers should also ensure that all equipment connected to electrical power is outfitted with surge protectors.

1.08.3 LOCKING WORKSTATIONS

When a customer leaves their workstation, even if it is only for a few moments, the customer should lock the workstation by pressing the ALT + CTRL + DELETE keys at the same time and then pressing ENTER. When the customer returns, the customer will need to press the ALT + CTRL + DELETE keys at the same time and then type their network login and password to access their system again. Doing this secures the system without losing any of the information the customer was working on at the time.

Customers should secure their equipment when leaving for the day by logging off or turning off all desktop computers, monitors and other devices connected to the Augusta network.

1.08.4 ACCESSING LOCKED WORKSTATIONS

Information Technology will not override a workstation login currently locked by a customer. Doing so can cause loss of data for the customer as well as data and program corruption. The ONLY exception to this will be when the workstation is compromised and is a security risk to the network. Even then, Information Technology personnel will attempt to contact the customer immediately to log into the workstation. If contact with the customer is unsuccessful in a network security risk situation, IT personnel will only disconnect the network cable from the computer until the risk can be contained. If you have any questions about this, please contact Information Technology's Security Administrator.

1.08.5 RECOVERING DATA FOR ABSENT OR TERMINATED EMPLOYEES

Any requests for files, contact lists, etc. should be made directly to the employee by the supervisor. If an employee is terminated, resigns, or retires, the employee's immediate supervisor must request a copy of all pertinent data prior to giving the employee their last check. All data must be examined for accuracy and completeness once it is received. Employee data should be treated in the same manner as all other property of Augusta.

If the department requires access to employee emails or information for a terminated employee, the Department Director must submit a request in writing to the Chief Information Officer or designee. See section 1.05.6 of the Email and Internet Communications policy. ***Once Information Technology receives a termination notice from Human Resources, all data will be removed (unless a retention request has been made).***

Whenever possible, information essential for operations should be stored in a location that is accessible by at least one backup employee (i.e., SharePoint or a shared drive). Similarly, backup access should be established for online systems and platforms. This practice prevents access issues delays when employees are out of the office for extended periods.

With appropriate planning and staffing backup protocols in place, most issues can be resolved without breaking security policies. Information Technology is always willing to work with departments to develop a workable solution so that operations can continue without interruption. Please contact Information Technology to discuss any concerns you may have.

1.08.6 EXCEPTIONS

Any exception to this policy will require a written request to Information Technology. The request must outline the data being sought, an explanation as to why the data was not retrieved prior to providing the employee with their last check, and a contact name and number for the person coordinating the data retrieval. Information Technology will review the request and work with the requesting department to identify a solution, if possible.

1.09 Standards for Augusta Web Pages and Social Media

1.09.1 PURPOSE

This policy governs documents (web pages) appearing on the Internet from Augusta servers, including the official Augusta website, as well as official Augusta accounts on social media platforms. These guidelines emphasize the need to maintain a high level of professionalism and consistency in how Augusta presents itself to the public. Augusta Information Technology is not responsible for third-party pages developed and hosted by external vendors.

1.09.2 RESPONSIBILITY AND GENERAL GUIDELINES FOR CONTENT

All official Augusta websites and social media accounts are considered extensions of Augusta's information networks. As such, they are governed by all Augusta policies regarding use of network resources and Internet communications. Departments that post content to the Internet or social media are responsible for complying with applicable federal, state, and county laws, regulations, and policies. This includes adherence to laws and policies regarding copyright, use of photographs, records retention, personnel privacy, public records, First Amendment, HIPAA privacy, the Americans with Disabilities Act, and information security policies established by Augusta.

Those who publish web pages or maintain social media accounts on behalf of Augusta shall take full responsibility for what they post. Employees must not use Augusta web pages or social media sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Inappropriate use of Augusta-related web pages or social media can be grounds for disciplinary action.

At a minimum, the following content guidelines must be followed for Augusta-hosted websites or social media accounts:

1. Departments and individuals shall not post any libelous or deceptive information. If such content is posted, both Augusta and the individuals responsible for publishing the information may be held potentially liable for such content.
2. Departments and individuals shall not post any material that is sexually explicit, obscene, or otherwise offensive. In general, Augusta's sexual harassment policy prohibits the display of sexually explicit material that interferes with anyone's work performance or creates an intimidating, hostile, or offensive environment. Creating and distributing (linking to) obscene content may also violate the law.
3. To reproduce copyrighted pictures or other copyrighted content on a web page, Augusta must have the copyright owner's permission. It is not sufficient to reproduce the owner's copyright notice; departments must actually obtain permission to reproduce the content, just as if the material was being published in a newspaper.
4. Employees administering social media platforms should be aware of the Terms of Service (TOS) of each platform. Each has its own unique TOS that regulates how users interact using that particular form of media. Any employee using a form of social media

on behalf of an Augusta department should consult the most current TOS in order to avoid violations.

1.09.3 COMMERCIAL USES NOT PERMITTED

Individual employees and departments shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on Augusta web pages or social media accounts. No paid advertising or marketing messages for non-Augusta entities may be published on Augusta's communications resources without coordination with Information Technology and approval by the Augusta Commission.

1.09.4 OFFICIAL AUGUSTA SOCIAL MEDIA SITES

Augusta departments have varying needs for the use of social media, depending on the specific services they offer. With the guidance of the Public Information Manager, each department that chooses to use social media as part of its business operations is responsible for managing its own social media presence and must adhere to the following guidelines.

1. Each department must designate a primary and secondary administrator for each social media account. These administrators must collaborate with the Public Information Manager and Information Technology to ensure their social media sites are consistent with other Augusta sites and brands.
2. Departments must secure (or set privacy settings for) each of their social media sites, so that only assigned employees can post to the site. Site administrators should take appropriate steps to minimize security risks to prevent fraud or unauthorized access to social media sites. Administrators are strongly advised to use different passwords for different accounts, since using the same password for all accounts increases the likelihood of accounts being compromised. Administrators should also change their passwords on at least a quarterly basis.
3. Communication on official Augusta social media platforms is considered a public record. Posts of the account administrator and any feedback by other employees and non-employees, including members of the public, will become part of the public record. Departments are responsible for retaining these records in accordance with the records retention schedule.
4. Active social media platforms should have new content posted frequently. Departments should closely monitor the analytics available for each social media site and use this information to develop a content management strategy.
5. It is strongly recommended that new information or updates be posted on both the Augusta website and any social media sites. Always provide links back to Augusta's official website for more information, forms, documents, or online services necessary to conduct business with Augusta.

1.09.5 REQUESTS FOR CONTENT CHANGES TO AUGUSTA WEB PAGES

Each department will maintain a primary and secondary contact person for their presence on the official Augusta website. These two web contacts and the Department Director will be the only people allowed to request changes for their department web site. The designated Web contact should adhere to the following guidelines.

1. All content changes will be submitted via email to the Web Administrator address (webadmin@augustaga.gov). Use of this address is important as it ensures that all changes and updates are distributed to several people, instead of just one individual.
2. The turnaround time for content changes is one to three days, depending on the size of the update. Some large updates may take longer. Turnaround time for email forms and script changes is one week. Please ensure requests are submitted with adequate time to fulfill it.
3. Departments must be explicit about describing content changes and the page to be updated. Vague or incomplete requests will result in delays. Include the page name and actual URL or address of the page in submissions.
4. Departments can also make changes and corrections by printing out the pages and marking them up with a red pen. Corrections can be scanned in and sent by email or sent through interoffice mail.
5. Department Directors must notify Information Technology if there is a change in their designated web contact personnel.

1.09.6 LIVE EDITING IN A STAGING ENVIRONMENT & TEMPLATES

Any department that is granted ‘live editing in a staging environment’ capabilities for the Augusta website must use the provided templates to do so. Templates and live editing are only available to departments who meet the necessary criteria.

- Have justified and relevant reasons to edit live content.
- Have a knowledgeable webmaster.
- Have a need for live updating due to legal requirements, etc.

The Augusta website uses Cascading Style Sheets. That means that font properties (type, size, and color) have already been specified. There is no need to specify fonts or heading sizes when making updates. Do not deviate from this standard.

Once the editing is completed in the staging environment, the Web Administrator will review and move the data to the production site.

1.09.7 AUGUSTA WEBSITE CONTENT RULES & STANDARDS

1.09.7.1 Filenames

All HTML files on the web site should be named in lowercase. Any spaces in the files should be substituted with the underscore character. This creates a cohesive and predictable naming environment that will make it easier to troubleshoot and manage the site. Other documents and images are not subject to the same rules and can be named as necessary.

1.09.7.2 Directory Structure

In order to maintain a logical and neat working environment the web site must conform to a standard directory structure.

- Standard navigation and design images will go in the root image directory.
- All departments and subsections of the web site will have their own directory under the departments' directory.
- Department directories will include folders for PDF files, specific department related images, and others for miscellaneous documents if needed.

1.09.7.3 Colors

The site will use standard colors to maintain design consistency. Consult the Public Information Manager or Web Administrator for the current color standards.

1.09.7.4 Images

Use of images or pictures on department sites should be limited by relevance to corresponding content. The following restrictions will apply.

- The webmaster may edit picture dimensions to fit the page properly.
- Pictures should maintain a small file size to ensure quick downloading. (Pictures that do not meet these requirements may be edited by the webmaster.)
- Use of clip art and other hand drawn art is discouraged. This is done to maintain a professional look and feel.
- Animations are strictly prohibited unless otherwise stated.

1.09.7.5 Other Documents

To make the site easier to maintain, more accessible, and easier to archive, all forms, meeting minutes, legal documents, and applications should be converted to PDF format unless otherwise stated. Use of PDF format is advantageous for several reasons:

- PDFs ensure no editing of the documents will take place after release, as the content is fully protected and cannot be altered.
- PDFs are fully accessible to the disabled.
- PDFs are easier to maintain and update using desktop tools, eliminating wasted time converting content to HTML.

1.09.7.6 Accessibility Standards

To make the website more accessible to people with disabilities, it has been developed in line with Section 508 Disability Guidelines. These Guidelines place restrictions on how content can be presented. In order to comply, changes may sometimes be needed to ensure department content is acceptable. Content that needs revision may be edited by the Web Administrator or sent back to the department for revision.

1.09.7.7 External Links

External links are allowed, as long as they:

- Are approved by Information Technology and/or Administrator's Office.
- Are relevant to Augusta or department content.
- Do not correspond to a commercial entity that has no bearing on Augusta government (for example, Mike’s Tropical Fish has no relevance to Augusta government).
- Are professional in nature. No personal links or sites that promote unofficial groups and individuals.
- Are explicitly noted as external and no longer part of the Augusta web site.

1.09.7.8 Plain Language

Whenever possible, website content should be written in plain language that is easy for the general public to understand. Avoid jargon, unnecessary technical terms and acronyms whenever possible. Content authors should use online readability tools to check that content is at roughly an 8th-grade reading level.

1.09.8 NOTIFICATION OF MAINTENANCE & CHANGES

Notification will be sent out to department web contacts in the event of any major maintenance or change to the Augusta website that incurs significant downtime.

1.10 Confidential and Personal Information

1.10.1 PURPOSE

Augusta has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully abridged. All information stored in electronic format must be secure and available only to those entitled to access that information.

Each Augusta employee has a legal responsibility to protect the confidentiality of records and information in his or her possession. This policy outlines the general guidelines for managing access to confidential and personal information.

1.10.2 SECURE ACCESS TO CONFIDENTIAL INFORMATION

Access to confidential information is intended only for legitimate Augusta use related to job responsibilities and roles within the Augusta department. “Need to know” is the basic principle. This information may not be released to any third party without proper authorization.

Customers shall not place confidential information in computers without properly protecting it. Augusta cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by a computer unless special arrangements are made. The nature of some departmental operations requires that access to personal data on employees and citizens be utilized. However, proper procedures must be followed prior to any prohibited information being downloaded to portable devices.

1.10.3 USE OF EMAIL

Ordinary electronic mail is not private. Do not use it to transmit computer passwords, credit card numbers, or medical information. Bear in mind that some records are required by law, and by Augusta policy, to be kept confidential. It is also necessary to protect confidential information about employees, such as performance evaluations.

Employees shall have no expectation of privacy associated with email transmissions and the information they publish/store on the Internet using Augusta’s resources.

1.10.4 PERSONAL INFORMATION

Excessive personal use of Augusta’s email or Internet resource shall lead to loss of the privilege to use them. Employees should not download any personal data, including social security numbers and any other prohibited information, onto Augusta-issued portable/mobile devices (laptops, smartphones, USB drives, etc.).

1.10.5 OPEN RECORDS ACT

Employees should be aware that the Georgia Open Records Act (O.C.G.A. § 50-18-70 through 50-18-76) applies to information stored in computers. This act gives citizens the right to obtain copies of public records, including any record prepared, received, or maintained by Augusta in the course of its operations. Data which is exempted from disclosure under the Freedom of Information Act (Public Law 93-502) or whose disclosure is forbidden by the Privacy Act (Public Law 93-579) will not be transmitted over the Internet network unless encrypted. All mobile law enforcement devices and GCIC/NCIC transmissions are encrypted.

1.11 Cooperation with Investigations and Open Records Requests

1.11.1 PURPOSE

The purpose of this policy is to establish guidelines for employee cooperation with investigations or requests brought by any agency or individual pursuant to the Georgia Open Records Act (O.C.G.A. § 50-18-70 through 50-18-76), or with any investigations initiated by a Department Director.

1.11.2 FULL COOPERATION

The Information Technology Department shall cooperate fully with any investigation or Open Records Act request that involves the use of computer equipment or the Augusta network by any customer. Augusta reserves the right to turn over any evidence of illegal or improper activity to the appropriate authorities.

1.11.3 NO EXPECTATION OF PRIVACY

Customers should not have any expectation of privacy with respect to their use of Augusta systems and equipment. All messages or files composed, sent, or received in the system are, and remain, the property of Augusta. They are not the private property of any employee. It is possible for deleted documents and messages to be recovered. Emails, Internet activity history, and any other electronic files are subject to retrieval.

In addition, Augusta may conduct electronic monitoring of employee activity without prior written notice.

See 1.05 Email and Internet Communications Policy for more information about employee privacy and record retention requirements. See 1.03 Computer Acceptable Use Policy for more information about electronic monitoring.

1.11.4 REQUESTS FOR INFORMATION

1.11.4.1 Internal Requests

Any Augusta Department Director or Elected Official seeking internal technology-related records must submit a written request through the Augusta Law Department. Information Technology will gather the information as requested. Information Technology will then release the collected information to the Augusta Law Department, which will determine which information is subject to disclosure to the requestor.

1.11.4.2 All Other Requests

Any other individual or agency seeking technology-related records must follow the Open Records Request process managed by the Administrator's Office. Information Technology will gather the information as requested. Information Technology will then release the collected information to the Open Records Officer for review and delivery.

1.12 Mobile Devices

1.12.1 PURPOSE

This policy shall apply to all Augusta employees, elected and appointed officials, and any other person authorized for the use of an Augusta-provided mobile device, the reimbursement for the use of a personal mobile device, or the use of a personal mobile device in the conduct of Augusta business.

1.12.2 AUTHORITY FOR APPROVALS

Department Directors/Elected Officials and their designees have authority to approve, deny or terminate the use of an Augusta-provided mobile device, the reimbursement for the use of a personal mobile device, or the ability to forward Augusta data to a personal mobile device.

1.12.3 USE OF AUGUSTA-ISSUED & PERSONAL DEVICES

Augusta shall take necessary measures to manage the use of Augusta-provided and personal mobile devices used in the conduct of Augusta business. Augusta is not responsible for the loss of personal information or costs that may result from the management and control activities needed to ensure the acceptable use of such devices. Any employees who access Augusta information from their personal devices do so at their own risk.

If an employee is issued an Augusta-provided mobile device, the device is the responsibility of that employee. The employee will be expected to pay the replacement cost of the device in the event of loss, damage or theft. See Section 1100.3, Loss Prevention, of the Personnel Policy & Procedures Manual for more information.

Random audits of mobile devices will be conducted.

1.12.4 EXPECTATIONS OF EMPLOYEE CONDUCT

All employees and elected and appointed officials conducting Augusta business on mobile devices are expected to comply with all Augusta policies and exercise the same care in communicating information as when communicating from any other Augusta-owned device.

Employees are expected to exercise good judgment while using the mobile network. Mobile devices are susceptible to monitoring and are not suitable for communications where privacy or security is a requirement. Mobile devices should not be left accessible to others (for example, in an unlocked car or on a desk).

Employees are expected to practice safety while using mobile devices. Mobile devices should not be used while the employee is driving, walking, biking, etc.

1.12.5 REASSIGNMENTS & EMPLOYEE SEPARATION

Mobile devices should not be transferred to individuals within departments without notifying the Information Technology Department. Mobile device changes and reassignments must be made through the Telecommunications Administrators, who can be contacted via the IT HelpDesk at 706-821-2524 or HelpDesk@AugustaGA.gov.

If an employee leaves the organization, their device should be turned into IT to be wiped and prepared for reuse. Departments are responsible for requesting service to be terminated for devices that will not reassigned.

1.12.6 COMMISSIONER DEVICES

On November 4, 2020, the Augusta Commission approved a policy allowing outgoing commissioners and mayors to purchase their respective cell phones and tablets after their last day in office. If an outgoing official wishes to purchase their device, they or the Clerk of Commission should notify their project manager in Information Technology.

Information Technology will calculate the current value of the equipment using straight-line depreciation of the initial purchase price over five years with a final salvage value of $0.00. Information Technology will provide this depreciation schedule to the Finance Department for review and approval. The officials will pay the calculated value of the equipment.

Information Technology will remove any Augusta applications and data from the devices and reset them to factory settings before releasing to the officials.

1.12.7 RESPONSIBILITY

The responsibility for ensuring compliance with this policy rests with each Department Director.

1.13 Radios

1.13.1 PURPOSE

All industry-standard radio-operating procedures are to be followed when using radios supplied by Augusta. Radios are to be utilized for Official Business Only. As each radio is issued an electronic ID number, which is printed to a computer every time the talk button is keyed on a radio, said unit will be identified each time the radio is used.

The Radio System Manager will provide support in ordering new radios, programming radios, having radios and other communication equipment repaired, and overseeing the entire communication system's operation in Augusta. By doing this, Augusta will be able to maintain standardization for the communication system.

1.13.2 ORDERING NEW OR REPLACEMENT RADIOS

The Radio System Manager will be responsible for ordering all of Augusta's communication equipment, ensuring the proper equipment is ordered and compatible with the existing system. When new or replacement radios are needed, a written requisition, with the appropriate department org key and object code, should be sent to the Radio System Manager. The Radio System Manager will review the requisition, ensuring all items are on the requisition with the most current state contract pricing.

1.13.3 PROGRAMMING PORTABLE RADIOS

All portable radios must be programmed through Augusta Communications to ensure that all of the correct information is in the radio. Individual I.D. numbers must be obtained from Augusta Communications, allowing the radio to operate on the Augusta system and ensuring that system integrity is maintained by having one person program the equipment.

1.13.4 REPAIR OF COMMUNICATION EQUIPMENT

The radio system and its components are under warranty with Motorola to maintain all of the communication equipment. Any piece of radio equipment requiring maintenance must route through Augusta Communications – if this is not possible, the Radio group in Information Technology will facilitate the repair.

1.13.5 PROPER USE OF COMMUNICATION EQUIPMENT

The Radio System Manager will be responsible for the proper use of the communication equipment. Any person improperly using the communication equipment, such as violating F.C.C. regulations, will be notified of the violation, and their Department Director will be made aware of the violation. Should improper use of the system continue, that person would not be allowed to operate any communication equipment owned by Augusta.

1.13.6 LOST OR STOLEN EQUIPMENT

Users who have lost or stolen equipment should immediately report the incident to the Radio System Manager and to Risk Management. The Radio System Manager will take the necessary steps to disable the unit to prevent any use by anyone not authorized by Augusta.

1.13.7 OBTAINING NEW I.D. NUMBERS

The only person authorized to obtain new I.D. numbers for the communication equipment is the Radio System Manager via Augusta Communications. The correct accounting of the I.D. database by one person maintains its integrity, and in the event of radio loss or other incident, provides additional information from that radio.

1.13.8 TWO-WAY RADIO POLICIES

1. Radios are for Official Business Only.
2. Employees shall utilize authorized talkgroups only.
3. Programming changes are not authorized without the approval of the Information Technology Department.
4. No Hardware or Accessories will be added or altered except by Information Technology or authorized personnel.
5. Each Employee assigned a radio will be responsible for said unit and accessories, to include a replacement in the event of loss or damage due to negligence.
6. Any damage or loss must be reported immediately in writing to Information Technology and Risk Management. Replacement options are at the discretion of the Department Director.
7. The transmission of profanity on said radio is prohibited.
8. Sexually explicit communication is prohibited in any form while using said system.
9. No radios will be used as a scanner after hours except as authorized by the Department Director.
10. All transmissions will be kept as brief as possible.
11. All repairs and re-programming will be directed through Augusta Communications.
12. Said radio system and equipment are controlled and directed through Information Technology.
13. Emergency radio functions are reserved for life-threatening functions only.

As each radio is issued an electronic ID number, which is printed to a computer every time the talk button is keyed on a radio, said unit would be identified each time the radio is used.

In the event of a disaster, the Public Safety and other departments must use the Emergency Operations Talkgroups. All Augusta radios are equipped with the six (6) Emergency Operations Talkgroups, so each department has interoperability capabilities within Augusta.

Any violation of this policy shall be subject to the policy and procedures of the Augusta Government and associated disciplinary actions. Users or Department Directors shall direct any problems or questions concerning the system to the Radio System Manager.

1.14 Open Data Policy

1.14.1 PURPOSE

Augusta, Georgia ("Augusta") recognizes that citizens' access to their local government's information is fundamental to transparency and accountability, and that the proactive disclosure of data promotes citizen engagement with the operations of government. Therefore, the purpose of this policy is to provide uniform guidelines for the proper management and protection of data residing on Augusta's open data platform "Open Augusta" for reuse by our citizens and the general public.

1.14.2 POLICY

It is the policy of Augusta to ensure a consistent and consolidated approach to selecting, publishing and maintaining data on Open Augusta. Open Augusta is a single solution available to all Augusta Offices and Departments ("departments") for sharing their data with the public.

Augusta departments are each responsible for determining which of their datasets are suitable for publishing on Open Augusta. Departments should work in cooperation with the Information Technology Department to make their respective datasets publicly available via Open Augusta.

1.14.3 DEFINITIONS

- Data - A value or set of values that represents a specific concept or concepts. Data becomes information when analyzed and possibly combined with other data in order to extract meaning and provide context.
- Data Steward – Departmental staff member designated by a Department Director as responsible for maintaining one or more departmental datasets on the Open Augusta platform.
- Dataset - A collection of data. Most commonly, a dataset corresponds to the contents of a single database table, or a single statistical data matrix, where every column of the table represents a particular variable, and each row corresponds to a given member of the dataset in question.
- Open Augusta Portal - www.augustaga.gov/openaugusta (https://geohub-augustagis.opendata.arcgis.com/)
- Open Augusta Data – Data generated and maintained jointly, openly shared, and available to the public in accordance with public records laws.
- Open Data - Data made public and provided in a convenient, modifiable form such that there are no unnecessary technological obstacles to the use of the data. For purposes of this policy, open data is machine readable, available in bulk, and provided in an open format.
- Portals - A means, usually a technology application, for transmitting open data for use, reuse, and redistribution.

- Principles of Open Data - Principles that govern the approach that Augusta uses to make data open. See "Principles of Open Data" at the end of this document.
- Restricted Data - All data that Augusta is restricted from disclosing under state or federal law and all data that Augusta is permitted to withhold from disclosure under state or federal law and has elected to withhold from disclosure.

1.14.4 OPEN DATA PORTAL OVERSIGHT

Oversight of the Open Augusta Portal has been delegated to the Information Technology Department, and the Chief Information Officer shall determine the Open Augusta Lead. It will be the responsibility of the Open Augusta Lead or their designee(s) to:

- Maintain the Open Data Portal (Open Augusta).
- Assist Augusta departments with determining which additional datasets will be added to Open Augusta as needed.
- Advise departments on best practices for open data-related projects and the requirements of this policy.
- Assist in the implementation of open data projects.
- Enforce this policy.
- Approve publishing of all datasets to be released.

Information Technology will not be responsible for the validity of any departmental data.

1.14.5 DEPARTMENTAL RESPONSIBILITIES

Each Augusta department can choose to participate in the Open Data program and select datasets for publication. Departments must designate a data steward for each open dataset and provide the necessary contact information for the data steward(s) to the Open Data Lead. It will be the responsibility of each departmental data steward to:

- Determine which data may be relevant to the public and which departmental datasets will be added to Open Augusta.
- Coordinate with other departmental staff to approve, extract, transform, and load procedures for each open dataset, with the assistance of the Open Data Lead.
- Establish a data refresh schedule for all data to be published.
- Determine what restrictions apply to departmental data and ensure any open datasets comply with these restrictions (see "Restrictions on Data Publication" below).

1.14.6 DATA PUBLISHING PROCESS

- Open Augusta is a long-term, single solution source available to all Augusta departments. It is the appropriate portal for sharing any open datasets with the public.

- The Open Data Lead will work as the primary partner to any department needing assistance and guidance to publish and release data.
- The Open Data Lead will assist departments in determining when and in what format data will be published to Open Augusta.

1.14.7 RESTRICTIONS ON DATA PUBLICATION

- Data restrictions apply to all data that is restricted from disclosure under state or federal law. Data restrictions also apply to all data that Augusta is permitted to withhold from disclosure under state or federal law and has elected to withhold from disclosure.
- It is the responsibility of each individual department to determine what data should be restricted or released. As departments are the appropriate stewards and custodians of the data they maintain, it will be up to each department to determine whether its data is restricted or not.
- Nothing in this policy shall be construed to supersede existing requirements for review and clearance of information exempt from disclosure under the Georgia Open Records Act (O.C.G.A § 50-18-70) and other applicable laws, regulations, or judicial orders.

1.14.8 PRINCIPLES OF OPEN DATA

All Augusta open datasets should adhere to the following principles, with certain exemptions identified in this policy if necessary:

- Complete: All facets of the data are available (unless subject to valid privacy limitations, including sensitive or protected information).
- Accessible: Data is easily and freely accessed via a central open data portal, Open Augusta, and is provided in bulk when possible.
- Primary: Data is collected at the source, with the highest level of granularity (not in aggregate or modified forms).
- Timely: Data is available to the public in a timely manner, ideally as soon as it is collected ("real-time" data), but subject to standards related to quality assurance and internal schedules and processes that may affect the validity of the data.
- Machine-Readability: Data shall be collected and released in machine readable, open formats based on common data standards that may allow for bulk download through an automated processing interface (API) and compatible with existing Open Data storage platforms.
- License-Free: When possible, data will be made available at no cost and with an open license, with no restrictions on copying, publishing, distributing, transmitting, or adapting the information. Data will not be subject to copyright, patent, or trademark regulation. In certain situations, contractual obligations may require that certain data cannot be released except through the use of a license and proprietary means.

- Non-Proprietary: Data should be available in a format over which no entity has exclusive control, with an exception for data owned by a third party and licensed by Augusta where existing contractual obligations limit open formats.
- Documentation / Metadata: For all datasets hosted on the Augusta open data portal, the following metadata shall be provided:
    - Name of department responsible for maintaining dataset.
    - Name of dataset owner in the department where data originates.
    - Frequency of data update and date and time of most recent update, when applicable.
    - Clear labels and explanations of data in each field.

1.15 Employee Security Awareness Training

1.15.1 PURPOSE

A robust cybersecurity framework for Augusta must include both technology-centered and human-centered strategies. Experience-based training is essential to help employees avoid security threats targeting sensitive data. This policy establishes guidelines for Augusta's employee security awareness training program.

1.15.2 POLICY & PROCEDURES

1. All new employees with network access must complete online security awareness training within the first 7 days from their date of hire.
2. All employees with network access must complete security awareness refresher training annually. Information Technology will notify employees when training is assigned and track completion of the required modules.
3. VPN access will not be granted unless the employee has completed all required training.
4. Information Technology regularly conducts testing to assess employees' ability to recognize common security threats. If an employee fails a phishing test, he or she will be required to complete an additional refresher training module within 30 days.
5. Department Directors are responsible for ensuring that their employees complete required training. Reports of employees who have not met training requirements are available from the Security Administrator. Directors will be notified if employees do not complete training within the required timeframe.
6. **Employees who do not complete required new employee, annual, or refresher training may be subject to loss of network access.**
7. Additional role-based security training may be required for employees who handle particularly sensitive data (e.g., additional requirements under HIPAA, PCI-DSS, etc.). If a department identifies a need for more specialized training, Information Technology will assist the department in identifying suitable training options.

1.16 Augusta Mass Email Guidelines

Email is an efficient, cost-effective, and environmentally friendly way to communicate quickly with our staff. Non-strategic use of mass email, however, can reduce our productivity and hinder our ability to deliver and recognize critical messages. It is our overall goal to ensure mass email remains an effective form of communication for all Augusta departments. For this reason, Augusta has two distinct mass email channels with different purposes:

- Augusta Notice
- Augusta Announcements

1.16.1 SUBMITTING A MESSAGE FOR DISTRIBUTION

For review and distribution, submit all mass email messages to the Administrator’s Office by sending the email directly to the Public Information Manager, any other designee in the Administrator’s Office, and to the following email address: **augannouncements@augustaga.gov** (note there is an “s” at the end of “announcements”). The Public Information Officer or designee will determine whether Augusta Notice or Augusta Announcement is more appropriate for the specific message.

1.16.2 AUGUSTA NOTICE

Augusta Notice mass email is used for information that pertains to the *majority of the recipients* and is *critical or time-sensitive.* For this reason, the use of Augusta Notice is limited. Examples of the types of emails appropriate for Augusta Notice include:

- Alerts to staff to situations about health and safety risks and emergency situations. (For example: facility closure due to a developing weather situation; loss of water, air conditioning or heating in a major facility; an active shooter situation.)
- Information essential to the operation or execution of business. (For example: a network outage or loss of internet connectivity.)
- Notifications to staff about changes in policies and practices. (For example: changes made to retirement benefit plans or the VPN policy.)
- Important information from the Administrator or his/her designee.

Exceptions could include urgent messages related to health and safety or business operations, which the respective department director would review prior to distribution.

Due to the types of messages specified above, the only offices with capability of distribution via Augusta Notice are the Information Technology Department, Augusta Emergency Management Agency, and the Administrator’s Office.

1.16.3 AUGUSTA ANNOUNCEMENTS

Augusta Announcements mass email is used to provide staff with information that might not be as time-sensitive or critical to staff's attention. This category of information would include, but not be limited to:

- Fundraisers (For example: United Way, American Heart Association HeartWalk, etc.)
- Retirement parties
- Monthly employee newsletter
- Safety tips from Risk Management.

1.16.4 MASS EMAIL BEST PRACTICES

To promote security, network efficiency, and readability:

- A mass email message should be brief, self-explanatory, clear, and concise—ideally under 200 words.
- Include a succinct subject line that conveys the email's purpose.
- Provide a link or contact information for those who might have questions.
- Avoid sending frequent or repeated messages. The only messages that should be exempt from this guideline are emergency communications for staff.
- Do not include attachments. If you have a graphic that complements your message, copy and paste the graphic into the body of the email.
- Avoid unfamiliar acronyms and jargon, which can be confusing and lead to misunderstanding.
    - Never use an acronym on first reference in the body of a message. If you must use a commonly understood acronym, spell it out in the first reference with parenthetical use of that acronym. For example, "…the Richmond County Sheriff's Office (RCSO)…" would be appropriate in the first reference, using RCSO on subsequent references.
- Always check spelling and grammar before submitting a message for mass email distribution.