BGSU
BOWLING GREEN STATE UNIVERSITY

3341-6-6 BGSU E-Mail Account.

Applicability	All University units
Responsible Unit	The Vice President for Finance and Administration
Policy Administrator	The Office of the Chief Information Officer

(A) Policy Statement and Purpose

ITS will only issue email accounts to individuals that meet the eligibility requirements. ITS will only issue one personal email account to each eligible individual.

ITS is responsible for issuing official BGSU email accounts. ITS has established eligibility requirements for email accounts to manage and secure the computing environment. By limiting account privileges to people that meet the eligibility requirements, ITS is better able to allocate resources to individuals actively working on university projects. ITS is also better able to identify and locate people that have misused computing facilities.

(B) Policy

An individual must have a current affiliation with the university. Affiliations include university employees (faculty and staff), currently enrolled students, retirees, Alumni and guests. Guest account requests are evaluated by ITS on a case-by-case basis.

An individual must acquire a BGSU authentication account prior to requesting other server accounts.

An individual must agree to abide by the policies and responsibilities outlined in the university's Acceptable Use Policy.

(1) Email Addresses

ITS has rules and standards for email usernames and the corresponding email addresses.

(a) Background

Individuals can acquire an email account upon meeting university affiliation requirements. When registering for an email account, the client must choose a username. This username will be used for all server accounts (including email) that the individual requests throughout his or her affiliation with the university.

Different server systems have different username requirements. Due to the broad use of this username, ITS has established rules and standards for usernames to meet the requirements of the various university server systems.

(b) Details

Individuals requesting an email account will choose from a list of available usernames. These usernames will be derived from the client's first, middle, and last names. The requestor must select a username from the choices provided. ITS will not accommodate requests for special or "vanity" usernames.

Usernames will not be available for selection by new subscribers until the previous owner's email account has been deleted for at least three months. This is done to help avoid confusion when messages meant for the original owner of the username are sent to the new owner.

If a client leaves the university for an extended period and his or her account is terminated, ITS cannot guarantee that the account username will be available if that client returns to the university at a later date.

(2) Username Changes

ITS will only change a client's username when a client has legally changed their name. This also changes the client's username for other server accounts.

(a) Background

As part of the email account acquisition process, a client is required to choose a single unique username from a list of available options derived from their first, middle and last names. This unique username is then used as the account name for every server account provided to the client. To minimize administrative overhead and to assure accurate record keeping, ITS has established strict rules for initiating a username change.

(b) Details

ITS will accept requests for changing a client's username if the client presents ITS with proof of a legal name change. The client should have their name changed on the Administrative Computer Systems (Human Resources and/or Student Information System) before requesting a username change. ITS will then process the username change and change all server account names assigned to that client.

ITS cannot change an individual's name on the Administrative Computer Systems. The client must make this request through Registration and Records

(3) Office Accounts

Departments and offices can obtain office email accounts for business correspondence. Multiple individuals within the department can access these accounts to process the incoming mail.

(a) Background

The university provides email as a tool for conducting the business of departments, academic offices, and ultimately

the university. Office accounts are intended to streamline the operations of departments and offices by providing accounts for group use. These accounts allow multiple individuals within a department to access and respond to incoming mail. These office accounts also allow the departments to advertise an email address that corresponds to a department or function, rather than an individual. These accounts are intended to minimize the impact of staffing changes and absences and eliminate the need for one person to access another individual's email account to perform university business.

(b) Details

Offices and Departments can obtain office email accounts by submitting a request to the ITS Technology Support Center. The requesting office or department will need to choose a name for the account (preferably eight to twelve characters long) that is not already in use.

Office accounts have the same restrictions and quotas as faculty and staff email accounts and can be accessed through Webmail and other POP and IMAP mail clients.

ITS has the right to limit the number of office accounts granted to a department or office.

(4) Email Forwarding

The owner of a BGSU E-mail account can have the account forwarded to an email address outside of the BGSU domain.

(a) Background

Clients must register for a BGSU E-mail account to acquire other server accounts. ITS recognizes that many individuals already have email accounts when they join the university community. To simplify management of individual's email accounts, ITS allows BGSU E-Mail accounts to be forwarded to an email address outside the BGSU domain.

(b) Details

ITS will not allow email to be forwarded from an individual's BGSU E-Mail address to another individual's BGSU email address.

ITS will immediately remove any forward that is suspected of creating an email routing loop or other delivery problems.

(5) Quotas on attachments

ITS will establish and enforce quotas on email attachment size provided to account holders. When an attachment is over its twenty-five Meg size, the email will not be delivered.

(6) Email Blocking

ITS reserves the right to block any incoming email messages that might cause email server problems, problems for the email users, or problems for the university's network.

(a) Background

Email can be used to transport virus-infected files or programs that can disrupt the email servers and the email user community. Email can also be used to broadly deliver information that is inappropriate or a nuisance (unsolicited bulk email, also known as "spam.") To protect the university community and university resources from such threats, ITS may block specific messages, senders or domains from the university's domain. These blocks may be set on a temporary or permanent basis depending on the nature of the threat.

(b) Details

ITS may use anti-virus software to automatically block messages that appear to be infected by a virus.

ITS may use “black-hole” lists to protect against known email abusers and sites with open relays. At times, legitimate senders may be blocked if they are sending from a site that has left itself open to abuse because of weak security.

ITS may manually set blocks on specific senders or domains when they are suspected of sending messages that are deemed inappropriate or a threat to our environment.

ITS will set size limits for email messages. The current maximum size for a single message is ten megabytes. Limiting the size of messages keeps individual accounts from exceeding their quotas and protects the university network from excessive traffic. Email messages that exceed the size limit will be blocked from entering the email server.

Email messages must properly identify the sender. Email messages that are found to not properly identify the sender will be blocked from entering the email server.

(7) Account Access

ITS reserves the right to restrict email server access methods to those appropriate for the intended use of a server. For security reasons, these methods are generally restricted to the lowest level of access needed to perform the intended functions of the server.

(a) Background

ITS is responsible for securing the university’s email environment. ITS evaluates the intended use of a server in conjunction with the security risks introduced by various account access methods to establish the best account access policy. In general, the least access necessary to provide the necessary services will be granted.

(b) Details

Email accounts can only be accessed with email software that follows Post Office Protocol (POP) or Internet Message Access Protocol (IMAP). Clients can use the ITS-provided Webmail interface to access their accounts, which uses the IMAP protocol to access the servers.

(8) Client Responsibilities

Account holders have responsibilities that must be met as part of the privilege of email access. Account holders are expected to live up to these responsibilities or lose their access privileges.

(a) Background

The email server environment is a shared environment. Since the account holders are a diverse group, and since email access is critical to university business, it is essential that each account holder use the servers responsibly.

(b) Details

An account holder is responsible for the use of his or her email account, and may not give anyone else access to that account. Conversely, account holders may not, in any way, try to obtain access any account other than their own.

An account holder is responsible for the security of his or her account password. This includes changing that password on a regular basis and ensuring that no one else knows it. It is also the account holder's responsibility to remember passwords that they set for their accounts.

An account holder may not deliberately perform acts that will disrupt the normal operation or diminish the performance of the network, servers, or other devices on the university network.

An account holder must abide by the terms of all software licensing agreements and copyright laws.

An account holder must abide by the rules established for the server where the account is housed. The account holder must follow all rules regarding quotas, server access methods, usage restrictions, etc.

An account holder must adhere to the responsibilities and policies dictated in Bowling Green State University's Acceptable Use Policy.

(9) Account Termination

BGSU accounts will be administratively disabled and deleted within an established time interval after the account holder is no longer affiliated with the university.

(a) Background

Information Technology Services has responsibility for managing access to the university's centrally controlled servers and services. Account termination policies have been established in order to enhance the security and reliability of these systems, and to allow for system resource planning and growth to meet the evolving needs of the university community. By limiting account privileges to users who have an active affiliation with the university, ITS can focus the resources and support toward the proper subscriber group and allow current and prospective students, faculty, and staff to get priority service.

(b) Details

Accounts held by individuals who violate university policies, policies established in the BGSU Information Technology Policy, or any ITS established policies will be immediately eligible to have their accounts administratively locked without prior notice.

Accounts held by student applicants who have failed to enroll and register for the term in which they were accepted for admission will be eligible for deletion the following term.

Accounts held by faculty and staff will be eligible for deletion ninety days after their resignation or termination, however retirees of BGSU are eligible to retain their email accounts indefinitely. Accounts of terminated employees may be administratively locked prior to the ninety day timeframe at the request of university administration or the management of the contracting department, area or unit. Faculty and staff must make arrangements prior to their departure from the university to publicize a new email address as appropriate.

Accounts granted to non-affiliated individuals (campus ministers, visiting scholars, adjunct (intermittent) faculty, external faculty, consultants, contractors, participants in Continuing Education courses or programs, etc.) will be considered eligible for deletion twenty-four months after their accounts are created. Individuals in this category who have a continuing role at the university can contact the Technology Support Center (TSC) when notified of their deletion eligibility to be put into contact with their sponsoring department, area or unit to request an additional twenty-four month extension of their access.

Accounts are eligible for deletion two weeks after the university has been notified that an account holder is deceased. Account privacy policies apply to all accounts, even after an account holder's death.

Accounts may be deleted at ITS discretion any time after they become eligible. A delay in the deletion process does not imply a right of the account holder to extended access to their accounts. Account holders can have their accounts deleted earlier than scheduled by placing a request through the Technology Support Center.

(10) Account Privacy

ITS will honor the account holder’s right to privacy. As necessary for email administration, ITS reserves the right to examine, log,

capture, archive, inspect, and preserve any messages stored on the university central servers.

(a) Background

ITS is responsible for managing and supporting the university email servers. This responsibility requires ITS to investigate and analyze server performance and security issues. At times, these efforts require ITS personnel to examine, log, capture, archive, inspect, and preserve messages in client accounts. ITS will honor the account holder's right to privacy except in cases where there are security violations, policy violations, and/or violations of the law.

(b) Details

Individuals eighteen years of age or older are considered to be adults in the State of Ohio and are therefore responsible for their own actions. ITS cannot honor requests from the parents of these individuals to release email account information or terminate email privileges for these individuals.

ITS employees are required to protect the account holder's right to privacy based on the confidentiality rules in the ITS Code of Ethics. Any violation by ITS employees of this code of ethics is considered grounds for dismissal.

Any email account that is associated with or suspected of being associated with security violations, policy violations, and/or violations of the law may be examined, logged, captured, archived, inspected, or preserved as part of a formal investigation. Any account found to be in violation may be turned over to university officials, law enforcement officials, officials of the court, or other officials engaged in an investigation.

(11) Public Records

Email correspondence that relates to the organization, functions, policies, decisions, procedures, operations or other activities of the university may be considered public documents under Ohio's Sunshine Laws. BGSU employees are responsible for maintaining these records. ITS does not assume responsibility to maintain archives of public record documents for its email clients.

(a) Background

ITS is responsible for managing and supporting the university email servers. This responsibility includes maintaining backups of the email system in case of catastrophic or system failures. These archives are expired on a regular schedule and only include messages that were in a client's account at the time of a backup. Our resources do not allow for a more extensive archive of public record documents of the type required by Ohio laws. Also, since personal correspondence is often mixed with business correspondence in BGSU email accounts, ITS disclosure of contents of email accounts in response to public records requests might also mean disclosing personal correspondence.

(b) Details

BGSU employees are responsible for maintaining records of correspondence that relates to university business. This includes electronic mail that may be subject to disclosure under Ohio's Sunshine Laws. ITS recommends that employees familiarize themselves with these laws and with BGSU's document retention policies and maintain their records accordingly.

Registered Date: March 17, 2015