Physical Facilities
Information Technology Services

Computer User Guide

March 27, 2010

Table Of Contents

Mission Statement and Goals

The mission of the Physical Facilities IT Services unit is to effectively and efficiently support the technological needs and infrastructure of the department. The IT Services unit strives to provide a high level of customer satisfaction; and works quickly to resolve reported IT problems.

The goals of IT Services include:

- To provide a single point of contact for IT-related problems within the department.
- To successfully resolve all reported IT problems in a timely, professional manner – or, to refer trouble-calls to Central Computing Services.
- To help employees use technology to the fullest extent possible through end-user training.
- To maintain the level of technical proficiency and expertise needed to resolve the majority of employees' IT problems.

IT Services is here to support YOU.

Technical Support

1. **A single point of contact**

   We serve as the primary contact for all problems related to Facilities computer & network systems. When applicable, we will refer problems to Central Computing Services.

2. **Desktop support**

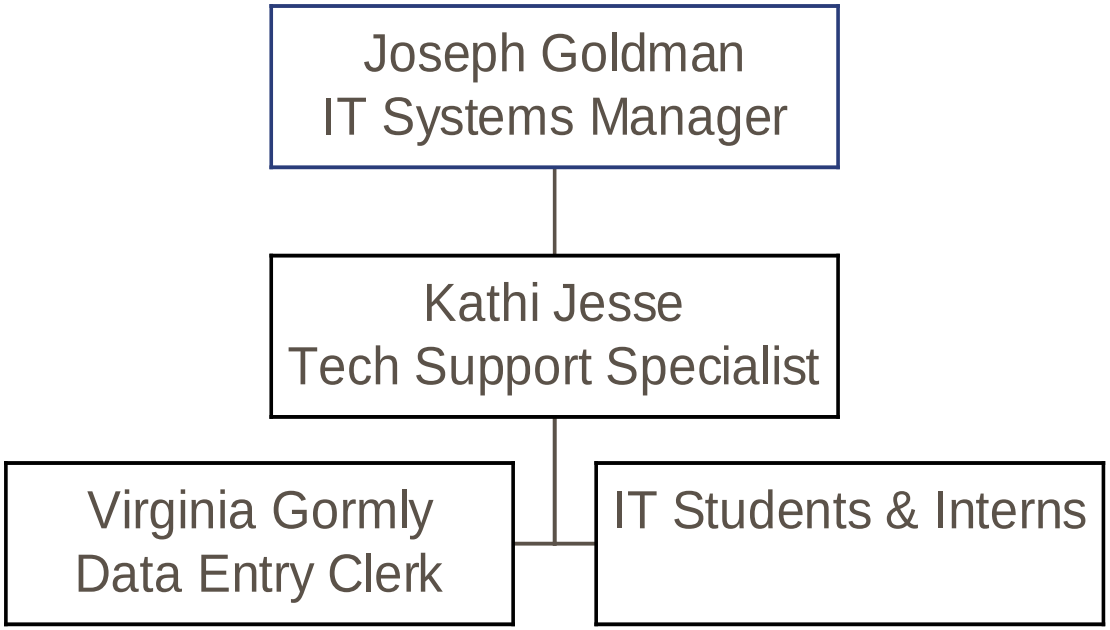
   We provide support for all State-owned computer hardware and software.

3. **End-user training**

   We can provide basic end-user training for staff, on standard business applications. Advanced training classes are held at the University Center for Training & Development. Refer to their website for schedules and information.

   http://training.binghamton.edu

IT Services Staffing



How to contact IT Services

1. **Telephone**
   - Kathi: 7-2899
   - Joe: 7-4483
2. **E-mail**
   - Kathi: KJesse@binghamton.edu
   - Joe: JGoldman@binghamton.edu
3. **In-person**
   - Kathi: Room 117, Physical Facilities
   - Joe: Room 116, Physical Facilities

IT Services hours of operation

- **During the Academic Semester:**

  8:30 AM to 5:00 PM (Monday through Friday)

- **During Summer Months:**

  8:00 AM to 4:00 PM (Monday through Friday)

Supported equipment and systems

The IT Services unit provides support for all University-owned technology:

- **Software and systems:**

  Operating systems, business productivity software, e-mail systems, and various proprietary systems.

- **Computer equipment:**

  Desktops, laptops, monitors, printers, keyboards, mice, PDAs, and all other peripherals; including PC projectors.

- **Network equipment:**

  Network cabling, hubs/routers/switches, servers, tape backup systems.

Unsupported equipment and systems

- Employee-owned personal computer systems and other electronic equipment and software.
- Office supply purchases: Copy machine/printer toner, storage media (floppy disks, CD-Rs or CD-RWs, magnetic tapes, etc.), video/audio cassettes, or batteries.
- Employee-owned pagers and/or cell phones.

Logging onto your computer

- To log onto your computer, use the User ID and password IT Services has created for you.
- The password does NOT expire – and you should not share your password with anyone.
- If you think your password has been compromised, contact IT Services and they will change the password for you.

Printer Connections

- Your computer has a default printer setup on it. This printer is located near your work area.

- There are a number of networked printers (monochrome and color) available for use. Contact the IT Services staff if you need assistance connecting to another printer.

Standard Software Installed

- Every Facilities computer has a “standard software setup” that includes:
  - Windows Operating system
  - Microsoft Office
  - Antivirus Software
  - Adobe Reader
  - Internet Explorer web browser

NOTE: *We have many more software applications licensed and available for your use. Contact IT Services for a more complete list.*

Email System

- As of March 2010, the campus moved to the Google Mail system, called “Bmail”. This is a web-based mail system, accessible from on and off campus. ***http://bmail.binghamton.edu***
- Central Computing Services will create your initial ID and password. You can change your password at any time.
- The mail system has an online Help system, that can answer your questions.

Network Calendar

- With the move to “Bmail”, the department also uses the built-in Google Calendar for meeting scheduling. ***http://calendar.google.com/a/binghamton.edu***
- You can access Google Calendar by using your “Bmail” login credentials.
- An online Help system is available to answer your questions about Google Calendar.

Work Management

- To manage work orders and projects, the department uses the FAMIS Work Management system.
- FAMIS is web-based, and you are provided with a logon/password credential to gain access.
- FAMIS training will be provided as needed; focusing on specific tasks you need to accomplish in the system.

Shared Network Storage

- We have shared network storage locations that you can use to store business-related files and data; rather than just on your hard drive.
- The drives are:
  - H: - The “H Drive” is the most common location you’ll store files to
  - X: - This drive is used primarily by the Design group, for drawings and designs

Technology Policies

- **Computer & Network Usage Policy:** Governs the use of information technology resources at the University.
- **Binghamton University Privacy Policy:** Governs how information provided by electronic “visitors” to the campus may be used.
- **Guidelines for Data Security:** Provides guidelines for handling & storing sensitive information.
- **Information Security Policy & Procedure:** Governs the use of sensitive and/or confidential information by University employees.
- **Software Support Policy:** Information on what levels of support the department’s IT Services staff provides.
- **Facilities Color Printing Policy:** Information about color printing support for department staff.

Binghamton University Computer and Network Policy

Last updated on Sep 21, 2007.

I. Introduction

Access to information technology is essential to the state university mission of providing the students, faculty and staff of the State University of New York with educational and research services of the highest quality. The pursuit and achievement of the SUNY mission of education, research, and public service require that the privilege of the use of computing systems and software, internal and external data networks, as well as access to the World Wide Web, be made available to all those of the Binghamton University community. The preservation of that privilege by the full community requires that each faculty member, staff member, student, and other authorized user comply with institutional and external standards for appropriate use.

To assist and ensure such compliance, Binghamton University establishes the following policy and the Binghamton University World Wide Web Policy which supplements all applicable SUNY policies, including sexual harassment, patent and copyright, and student and employee disciplinary policies, as well as applicable federal and state laws.

II. General Principles

1. Authorized use of Binghamton University-owned or operated computing and network resources shall be consistent with the education, research and public service mission of the State University of New York and consistent with this policy.

2. Authorized users of Binghamton's computing and network resources are defined as those individuals provided a username and password, for their own use only, through legitimate Binghamton University processes for assignment of such identification from Information Technology Services. An authorized use of Binghamton's computing and network resources is initiated by entering that individual's username and password. Using another individual's username and password is an unauthorized use. The only exception to this authorized use definition is access on designated computers provided in the University Library where use of a username and password will not be required.

3. This policy applies to all Binghamton University's computing and network resources, and external computing and networking resources accessed via Binghamton's computing and networking resources.

4. The University reserves the right to limit access to its networks when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated.

5. The University reserves the right to remove or limit access to material posted on university-owned computers when applicable campus or university policies or codes, contractual obligations, or state or federal laws are violated.

6. Non-University-owned computers which house material which violates the University's policies are subject to network disconnection without notice.

7. Although the University does not generally monitor or restrict the content of material transported across networks, it reserves the right to access and review all aspects of its computing systems and networks, including individual login sessions and account files, to investigate performance or system problems, search for viruses and other harmful programs, or upon reasonable cause to determine if a user is violating this policy or state or federal laws.

8. This policy may be supplemented with additional guidelines by campus units that operate their own computers or networks, provided such guidelines are consistent with this policy.

III. Acceptable Use

Privacy: No user should access, view, copy, alter or destroy another's personal electronic files without permission (unless authorized or required to do so by law or regulation). If another user has failed to close out their session a new user must close that session and enter their own username and password to use that computer.

Copyright: Written permission from the copyright holder is required to duplicate any copyrighted material, except where consistent with Fair Use. This includes but is not limited to duplication of music, audiotapes, videotapes, photographs, illustrations, computer software, data and all other information for educational use or any other purpose. Most software and databases that reside on the University's computing network are owned by the University or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the University's network or for distribution outside the University, against the resale of data or programs, or against the use of software for non-educational purposes, or for financial gain, and against public disclosure of information about programs (e.g., source code) without the owner's authorization.

Harassment, Libel and Slander: No user may use the University's computers or networks to libel, slander or harass any other person.

Sharing of access: Computer accounts, passwords, and other types of authorization are assigned to individual users and not shared with others. The assigned user is responsible for any use of the account. Sharing of a computer account constitutes an inappropriate use and may lead to termination of that account

Permitting unauthorized access: Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. Failure to configure hardware or software in a way that reasonably prevents access by unauthorized users is a violation of acceptable use.

Termination of access: When a user ceases to be a member of the campus community or is assigned a new position and/or responsibilities within the State University system, the user's access authorization must be reviewed. Users must not use facilities, accounts, access codes, privileges or information for which they are not authorized in their new circumstances.

Residence Hall Access: Residence hall access to the campus network is granted to individuals. Each individual is responsible for assuring that his/her personal residence hall room access point is not misused.

Circumventing Security: Users are prohibited from attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

Breaching Security: Activities which degrade the performance of a computer system or network, use a system or network for which the user is not authorized, or deprive authorized users of resources or access to computers or networks is prohibited.

Game Playing: Limited recreational game playing by students, which is not part of authorized and assigned research or instructional activity, is acceptable, but computing and network services are not to be used for extensive or competitive recreational game playing disruptive to others. Recreational game players occupying a seat in a public computing facility must give up the use of the device when others who need to use the facility for academic or research purposes are waiting.

Chain Letters: The propagation of chain letters is an unacceptable practice and is prohibited.

Unauthorized Monitoring: A user may not monitor the electronic communications of others.

Flooding: Generating excessive network traffic, including spamming and denial-of-service, is prohibited.

Private Commercial Purposes: The computing resources of Binghamton University shall not be used for private commercial purposes or for financial gain.

Political Advertising or Campaigning: The use of Binghamton University's computers and networks shall be in accordance with University policy on use of University facilities for political purposes (SUNY Administrative Procedures Manual Policy 008).

Modifying software or software installation: A user may not modify the software configuration on any computer provided for general access.

IV. Limitations on Users' Expectations *(User Cautions!)*

1. The issuance of a password or other means of access is intended to assure appropriate confidentiality of the University's files and resources and does not guarantee privacy for use of university equipment or facilities.

2. The University provides reasonable security against intrusion and damage to files stored on the central facilities, and provides for some archiving of files based upon the operational needs of the University. However, the University is not responsible for the loss of users' files or data. Users should take their own steps to backup and protect important information.

3. Users should be aware that the University's computer systems and networks might be vulnerable to unauthorized access or tampering. In addition, computer files, including e-mail, may be considered "records" which may be accessible to the public under the provisions of the New York State Freedom of Information Law.

4. Email messages are not personal and private. While administrators will not routinely monitor individual email and will take reasonable precautions to protect the privacy of Email, program managers and technical staff may access a student or employee's Email:

- For a legitimate business purpose (e.g. the need to access information when an employee is absent),
- To diagnose and resolve technical problems involving the system, and/or
- To investigate possible misuse of Email when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

5. Email messages sent/received in conjunction with University business may:

- Be considered state records under applicable state regulations;
- Be releasable to the public under the Freedom of Information Law;
- Require special measures to comply with the Personal Privacy Protection Law.

6. All Email messages including personal communications may be subject to discovery proceedings in legal actions.

V. Sanctions

Violators of this policy may be subject to immediate suspension of services by Information Technology Services and to the existing student or employee disciplinary procedures of Binghamton University. Sanctions may include the loss of network access and computing privileges. Illegal acts involving Binghamton University's computing resources may also subject users to subpoena and prosecution by commercial enterprises, local, state and/or federal authorities.

Privacy Policy

Last updated on Jul 7, 2006.

Binghamton University Commitment to Privacy

At Binghamton University (binghamton.edu) we are committed to protecting your privacy and making it easier and more efficient for individuals and organizations to interact with us. In developing this policy, Binghamton University adhered strictly to federal and state laws, rules and regulations, policies and procedures of the State University of New York and Binghamton University, specifically the provisions of the Internet Security and Privacy Act, the Freedom of Information Law, and the Personal Privacy Protection Law. We recognize that it is critical for individuals and organizations to be confident that their privacy is protected when they visit binghamton.edu. You can travel through most of binghamton.edu without giving us any information about yourself. Sometimes we do need information to provide services that you request, and this commitment of privacy explains our online information practices.

Binghamton University does not collect any *personal information* about you unless you provide that information voluntarily by sending an e-mail or by voluntarily completing a data collection instrument (i.e. survey, application, request for information) available through binghamton.edu

Information Collected Automatically When You Visit binghamton.edu

When visiting binghamton.edu, Binghamton University automatically collects and stores the following information about your visit:

- The Internet Protocol address of the computer that accessed our Web site.
- The type of browser, its version and the operating system on which that browser is running.
- The Web page from which the user accessed the current Web page
- The date and time of the *user*'s request
- The pages that were visited and the amount of time spent at each page.

None of the above-mentioned information is deemed to constitute *personal information* by the Internet Security and Privacy Act. The information that is collected automatically is used to improve binghamton.edu's content and to help Binghamton University understand how *users* are interacting with its Web site. This information is collected for statistical analysis and to determine what information is of most and least interest to our *users*. The information is not collected for commercial marketing purposes and Binghamton University is not authorized to sell or otherwise disclose the information collected from binghamton.edu for commercial marketing purposes.

Information Collected When You E-mail binghamton.edu or Complete a Transaction

During your visit to binghamton.edu you may send an e-mail to Binghamton University. Your e-mail address and the contents of your message will be collected. The information collected is not limited to text characters and may include audio, video, and graphic information formats included in the message. Your e-mail address and the information included in your message will be used to respond to you, to address issues you identify, to improve this Web site, or to forward your message to another Binghamton University campus server for appropriate action. Your e-mail address is not collected for commercial purposes and Binghamton University is not authorized to sell or otherwise disclose your e-mail address for commercial purposes.

During your visit to binghamton.edu you may complete a transaction such as an online survey, application or Information Request Form. The information collected by Binghamton University, including *personal information* volunteered by you in completing the transaction, is used by Binghamton University and may be disclosed by Binghamton University for those purposes that may be reasonably ascertained from the nature and terms of the transaction in which the information was submitted.

Binghamton University does not knowingly collect *personal information* from children under the age of 13 or create profiles of children under the age of 13. *Users* are cautioned, however, that the collection of *personal information* submitted in an e-mail will be treated as though it was submitted by an adult, and may, unless exempted from access by federal or State law, be subject to public access.

Disclosure of Information Collected Through This Web site

The collection of information through binghamton.edu and the disclosure of that information are subject to the provisions of the Internet Security and Privacy Act. Binghamton University will only collect *personal information* through binghamton.edu or disclose *personal information* collected through binghamton.edu if the *user* has consented to the collection or disclosure of such *personal information*. The voluntary disclosure of *personal information* to Binghamton University by the *user* constitutes consent to the collection and disclosure of the information by Binghamton University for the purposes for which the *user* disclosed the information to Binghamton University.

However, Binghamton University may collect or disclose *personal information* without consent if the collection or disclosure is: (1) necessary to perform the statutory duties of Binghamton University, or necessary for Binghamton University to operate a program authorized by law, or authorized by state or federal statute or regulation; (2) made pursuant to a court order or by law; (3) for the purpose of validating the identity of the *user*; or (4) of information to be used solely for statistical purposes that is in a form that cannot be used to identify any particular person.

Further, the disclosure of information, including *personal information*, collected through binghamton.edu is subject to the provisions of the Freedom of Information Law and the Personal Privacy Protection Law.

Binghamton University may disclose *personal information* to federal or state law enforcement authorities to enforce its rights against unauthorized access or attempted unauthorized access to Binghamton University's information technology assets.

Retention of Information Collected Through this Web site

The information collected through binghamton.edu is retained by Binghamton University in accordance with the records retention and disposition requirements of the New York State Arts & Cultural Affairs Law. In general, the Internet services logs of Binghamton University, comprising electronic files or automated logs created to monitor access and use of Agency services provided through binghamton.edu, are retained for 60 days and then destroyed. Information concerning these records retention and disposition schedules may be obtained through the Internet privacy policy contact listed in this policy.

Access to and Correction of *Personal Information* Collected Through binghamton.edu

Any *user* may submit a request to Binghamton University's privacy compliance officer to determine whether *personal information* pertaining to that *user* has been collected through binghamton.edu. Any such request shall be made in writing and must be accompanied by reasonable proof of identity of the *user*. Reasonable proof of identity may include verification of a signature, inclusion of an identifier generally known only to the *user*, or similar appropriate identification. The privacy compliance officer is also the University Counsel and the address is:

Office of University Counsel

Binghamton University AD-614

PO Box 6000

Binghamton, NY 13902-6000

The privacy compliance officer shall, within five (5) business days of the receipt of a proper request, provide access to the *personal information*; deny access in writing, explaining the reasons therefore; or acknowledge the receipt of the request in writing, stating the approximate date when the request will be granted or denied, which date shall not be more than thirty (30) days from the date of the acknowledgment.

In the event that Binghamton University has collected *personal information* pertaining to a *user* through binghamton.edu and that information is to be provided to the *user* pursuant to the *user's* request, the privacy compliance officer shall inform the *user* of his or her right to request that the *personal information* be amended or corrected under the procedures set forth in section 95 of the Public Officers Law.

Confidentiality and Integrity of *Personal Information* Collected Through binghamton.edu

Binghamton University is strongly committed to protecting *personal information* collected through binghamton.edu against unauthorized access, use or disclosure. Consequently, Binghamton University uses good faith efforts to limit employee access to *personal information* collected through binghamton.edu to only those employees who need access to the information in the performance of their official duties. Employees who have access to this information follow appropriate procedures in connection with any disclosures of *personal information*.

In addition, Binghamton University has implemented procedures to safeguard the integrity of its information technology assets, including, but not limited to, authentication, authorization, monitoring, auditing, and encryption. These security procedures have been integrated into the design, implementation, and day-to-day operations of binghamton.edu as part of our continuing commitment to the security of electronic content as well as the electronic transmission of information.

For Web site security purposes and to maintain the availability of binghamton.edu for all *users*, Binghamton University employs software to monitor traffic to identify unauthorized attempts to upload or change information or otherwise damage binghamton.edu.

Cookies

Cookies are small pieces of information that are stored by the *user's* browser on the hard drive of your computer. To better serve you, we occasionally use "session cookies" to enhance or customize your visit to this website.

Disclaimer

The information provided in this privacy policy should not be construed as giving business, legal, or other advice, or warranting as fail proof, the security of information provided through binghamton.edu.

Contact Information

For questions regarding this Internet privacy policy, please contact our privacy officer via e-mail at bwestbro@binghamton.edu or by regular mail at:

Office of University Counsel AD-614

Binghamton University

PO Box 6000

Binghamton, NY 13902-6000

Definitions

The following definitions apply to, and appear in *italics*, in this policy:

Personal information: For purposes of this policy, "*personal information*" means any information concerning a natural person, which, because of name, number, symbol, mark, or other identifier, can be used to identify that natural person.

User: shall have the meaning set forth in subdivision 8 of section 202 of the New York State Technology Law.

Guidelines for Data Security

Last updated on Jun 3, 2009.

It is the responsibility of all University employees and/or persons with access to University data to respect the highest level of privacy for their colleagues and other members of the University community.

New state laws require that the University report cases of intrusion into certain types of personal information to the person affected, and in some cases, to state agencies.

Steps Every User of Sensitive Information Should Take

Consider what information you store and where you store it.

- Do not store personally-identifiable information about others on your PC, even though it may be convenient to do so. The convenience of having the information on a PC may not be worth the risk of exposing someone else's identity to theft, and exposing you to the liability and bad publicity that may follow. Consider:
  - Does such information have to be stored on a PC at all?
  - If it has to be on a PC, how can it be most effectively protected?
  - Can it be stored on a server (NOT a web server) where it is more closely guarded?
  - Should the data be encrypted?
- Do not store sensitive information on web servers or other machines that are open to the public. Web servers themselves draw outside users, and provide security holes if they are not constantly patched and kept up-to-date. If you're unsure about this, please contact Information Technology Services.
- Do not take on the collection of sensitive information without authorization from the University's Information Security Council.
- Do not store sensitive information on departmental computers without authorization from the University's Information Security Council.

Control access to rooms and file cabinets where paper records are kept.

- Secure customer information behind locked doors when unattended
- Prohibit unescorted guests from areas where customer information is in plain view
- Dispose of documents containing customer information that are no longer needed in designated recycling/shredding containers.

Protect information stored electronically.

- Secure workstations behind locked doors after business hours
- Shut down your PC or minimize screens when not in use
- Lock computer workstations when leaving them unattended
- Don't allow anyone else access to your computer in your absence.
- Manage passwords wisely
  - Use strong passwords of 8 characters or more that don't spell common words and do mix numbers, small and capital letters and special characters
  - Change passwords every 60 days in systems hosting sensitive data
  - Do not post passwords near or on computers
  - Never give anyone else your login password, or any password.

- Password-protect and encrypt sensitive data files, if you have to have them at all.
- If your Windows 2000 or XP machine is not set up by Information Technology Services, make sure that the administrative password is NOT left blank
- Encrypt sensitive customer information when it is transmitted electronically over public networks.

Respond to requests for information about students in accordance with FERPA.

Report any fraudulent attempts to obtain customer information to management, who then report the attempt to the appropriate law enforcement agencies.

Security Concerns for PDF Reports on Firestone

In an effort to reduce paper consumption and increase efficiency, ITS had converted many “green bar” reports to PDF format and placed them in secured folders on Firestone for viewing.

With the growing awareness of the impact of security breaches, it has become clear that each of one of us needs to be aware of the content we save on our desktop and laptop computers. We have the responsibility to protect confidential and sensitive information about our students and staff members and to do it to the best of our ability.

Some reports on Firestone contain sensitive and confidential information. There are risks any time sensitive information is made available in a report. We must be aware of the risks and take every precaution to prevent a security breach.

It is possible to open the PDF file on Firestone and then save it to your desktop or laptop computer. By doing so, this increases the risk of the report ending up in the wrong hands.

Here are some do’s and don’ts when viewing the PDF reports stored on Firestone.

Do...

- View the reports from Firestone
- Close the PDF when it is no longer needed
- Delete old reports from your folder that are no longer needed

Don’t...

- Save the PDF file on your desktop or laptop machine
- Email the report to another colleague
- Create a shortcut to the report on your desktop
- Save the report on other media, like a flash drive or cd
- Print the report if it isn’t necessary
- Share your access information with anyone

We also recommend that you review files on your PC and remove any file that contains confidential and sensitive information, particularly files that may contain social security numbers.

If you have any questions or concerns, please contact the ITS Help Desk or your technical contact in ITS.

Frequently Asked Questions

I have Windows Updates enabled and am using the latest antivirus software. Is data on my PC protected?

You've made a good start, but your PC may not be protected. As new exploits are developed, there is a lag time between when antivirus and operating system patches can be modified and distributed by the vendors to protect against the new exploit. Also, new "spyware" threats are developed all the time, and antivirus software does not consistently target this potentially malicious code. Again, the only real protection is to isolate your PC from the network and unauthorized users.

My PC is password protected. Does that protect me from network intrusion?

No! The password only protects the machine from being booted up by someone who doesn't know the password. It does nothing to protect from network access.

What information is of particular concern?

Student data is protected by FERPA, and only information that is defined as "directory" information may be released about students, and even that may be restricted. Information about public employees in some circumstances is more public, but in all cases, information that could lead to identity theft must be protected. Information that can individually identify a person must be safeguarded, particularly the combination of name and social-security number, and personal information like marital status, etc.

If I need help, whom can I call?

Call your regular contact within Information Technology Services, if you have one. Otherwise, call the Helpdesk at 7-6420 to ask for an appointment to talk about this matter with our staff.

If I run a web server, how can I make it secure?

No machine can be made **immune from intrusion** if it is networked. Web servers are designed to be networked and to serve outside users, so they are especially vulnerable.

If your web site deals with sensitive information, you must "harden" the machine that hosts it to keep intruders from monitoring transactions or innappropriately gathering other users' private data. This "hardening" includes:

- frequently removing collected data so it is not stored there if the machine is intruded upon, and
- keeping the machine (the server and system software) patched and up-to-date to minimize the risk of intrusion.

Continual diligence and maintainance is required for the **full life-cycle** of server operation.

Some tools for checking the security of "apache" web servers are available for Educause members (which includes Binghamton) at The Center for Internet Security at <http://www.cisecurity.org/> (just be sure to register in accordance with the Educause Member agreement, explained there). You can also contact Information Technology Services for help.

Information Security Policy and Procedure

Last updated on Jun 3, 2009.

Binghamton University, State University of New York

Approved April 24, 2006

SUBJECT:

Confidentiality of Student and Employee Records and other University-Maintained Data

STATEMENT OF POLICY:

As a general principle, without reasons to the contrary, Binghamton University will make available to our employees, data that are necessary to allow them to fulfill their official University work assignments. As a result, selected staff and faculty members handle a variety of protected (proprietary and private) information concerning colleagues, students, parents, alumni, donors, and others associated with the University, as well as confidential information regarding University business. This material may include (but is not limited to) personal data such social security numbers and home addresses, donor files, student records, or University financial information. The University will adhere to all appropriate state and federal laws. The Information Security Council has been established to oversee and coordinate information security at Binghamton University. Members of the committee are:

- Information Security Officer (Chair)
- Representative from each Division (5)
- Representative from each College (6)
- Representative from Library
- Representative from Graduate School
- Associate Vice President - ITS
- Associate Vice President - Administrative Services
- Director of Human Resources
- University Registrar
- University Council

Data and data types should be classified by their use and releasability; categories are open, restricted, and confidential. These are defined as follows:

1. Open: Public information about the University and its community releasable at the lowest department level (e.g. sports scores, public events information, announcements, faculty expertise, student accomplishments, aggregate data prepared for release).
2. Restricted: Public information subject to established University protocol for release (e.g. budget information, salaries, expenditures, directory information).
3. Confidential: All other information, including any personally-identifying information about employees or students. Note: Student directory information is confidential if a directory exclusion is requested by the student. It is the responsibility of all University employees to respect the highest level of privacy for their colleagues and other members of the University community. Disclosure and discussion of information obtained from University records, either during or after employment with the University, is not permissible unless such disclosure is a normal requirement of an employee's position or has been so authorized.

University employees or persons with access to University data shall not:

- Exhibit or divulge the contents of any record or report to any outside party or other University employee unless the latter requires the information to perform his or her work-related duties. When in doubt, an employee receiving a request should refer the matter as follows:
    - Requests for information about individual students should be referred to the Office of the University Registrar
    - Requests for information about individual employees should be referred to the Office of Human Resources
    - Requests for all other information about the University should be referred to the Office of Communications & Marketing
    - If additional clarification is required or in the case of broader policy questions, please refer the matter to the Chair of the Information Security Council
- Make unauthorized use of any information in files maintained, stored, or processed by Binghamton University, or permit anyone else to make unauthorized use of such information.
- Seek personal benefit or permit others to benefit personally from any information that has come to them by virtue of their work assignment.
- Knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.

SCOPE:

This policy applies to all members of the Binghamton University workforce, whether directly employed by the institution or serving under an alternative arrangement. It shall include, but not be limited to:

- Employees of Binghamton University, the Research Foundation, and the Binghamton Foundation (including teaching assistants, graduate assistants, and other student employees)
- Interns
- Volunteers
- Consultants
- Contractors and subcontractors

EXPECTATIONS:

Binghamton University expects all employees to be familiar with:

- The need for confidentiality
- The types of information that are considered confidential
- The institution's confidentiality policies and procedures

Binghamton University regularly reminds employees of their responsibility to protect confidential information.

CONFIDENTIALITY AGREEMENT:

Each member of the Binghamton University workforce will be expected to review and sign the University's Agreement to Protect Confidential Information. This signed statement will be maintained in the appropriate employee personnel file.

SUSPECTED BREACH:

All suspected breaches of this policy must be reported to the area/department supervisor who should immediately contact the Director of Human Resources or the Chair of the Information Security Council. Any violations of this policy may be cause for immediate termination of access to confidential information and may result in disciplinary action, including dismissal from employment.

To: All Binghamton University Faculty & Staff

From: Enterprise Data Committee - Stephen Gilje, Ellen Haley, Sylvia Hall, Jillian Harrington, Lloyd Howe, Terry Kelley-Wallace, Len Kogut, Dick McCarthy, Michael McGoff, Pete Partell, Mark Reed, Chris Ritter, Barbara Scarlett, Jennifer Schorr

Date: September 27, 2006

Re: Protecting Student, Faculty and Staff Data

Not a month goes by without news about an institution that has unintentionally jeopardized the identity of those whom it serves. Many times private information is compromised when employees of good intention are simply not aware they are leaving sensitive data unprotected.

Binghamton University values the security and good will of our students, faculty and staff and has established policies and guidelines to help everyone on campus protect private information. These policies are available online at the Computing Services website, as listed below. It is the responsibility of all University employees and/or persons with access to University data to respect the highest level of privacy for their colleagues and other members of the University community.

New state laws require that the University report cases of intrusion into certain types of personal information to the person affected, and in some cases, to state agencies. Please help us to avoid any reportable incidents by following University policies with regard to information security and privacy.

Additional information on these polices can be found at the Computing Services Website at:
http://computing.binghamton.edu/policies

Also, information regarding the Family Educational Rights and Privacy Act (FERPA) can be found at the Registrar's website at:
http://registrar.binghamton.edu/FERPAmain.htm

Following please find the ***Principles to Protect Confidential Information***, which provides further detail on the requirements of faculty and staff to protect sensitive information. It is expected that faculty and staff that supervise College Work Study students or other student workers with access to confidential information will share these policies and guidelines with those student workers.

If you should have any questions regarding this agreement, information security, or other privacy issues, please feel free to contact Jillian Harrington, chair of the Enterprise Data Committee at 7.2808, or via e-mail at jharring@binghamton.edu

Binghamton University
State University of New York

Principles for Protection of Confidential Information

It is the responsibility of all University employees and/or persons with access to University data to respect the highest level of privacy for their colleagues and other members of the University community. All persons with access to University systems are responsible for compliance with the University privacy policies (available online at http://computing.binghamton.edu/policies/).

Also, all persons with access are required to read, understand, and abide by the following principles:

- Although I may have broad access to student and/or employee information, I will access and use only that information that is necessary to perform my duties.
- I will not release confidential information from student or employee records, in any form, to any other party except in accordance with Binghamton University's applicable policies and procedures.
- When discussing confidential student or employee information with others for authorized purposes, I will exercise care to keep the conversation private and not to be overheard by others not authorized to have such access.
- I will maintain my network and computer personal IDs and passwords in confidence. I will not disclose them to any other person or authorize others to use them.
- I understand and agree that my obligation to maintain confidentiality will continue even after I leave the employment of Binghamton University.
- I understand that any violation of this agreement will result in immediate termination of my access to online confidential information and may also result in disciplinary action, up to and including dismissal.
- I understand that violation of this Agreement is a serious matter and that I may be held personally liable for claims which may arise from such violations.

1 March 2010

TO: All Physical Facilities staff

RE: Software support

In order to provide the highest level of software support we can, the Information Technology Services staff has developed this outline of Software Support Tier's.

The IT Services staff will provide support based on these tiers, for each software application obtained through NY State purchasing; and properly licensed to Physical Facilities/Binghamton University. Specific applications will be installed on the individual PCs, while other applications are run from the applications servers.

Software NOT PURCHASED OR LICENSES by Physical Facilities/Binghamton University, or tested by IT staff, will not be supported. Staff is encouraged to contact the IT staff before purchasing any software.

- Tier 1: Full Support – IT Services staff are responsible for installing, configuring, and upgrading the package. Basic training is available on campus.

- Tier 2: Basic Support – IT Services staff are responsible only for installing and configuring the package. Upgrades will be done at the user's request. Users are responsible for arranging their own training.

Supported applications Examples of software that is supported by the IT section:

Support Tier	Application or Operating System
1	Adobe Acrobat
1	BEST Keystone 600
1	FAMIS Maintenance Management
1	Google Applications System (Bmail, Calendar)
1	Kronos Time Management
1	MS Office (Word, Excel, PowerPoint, Access)
1	MS Windows
2	AutoCAD Applications
2	Gasboy System

Software installation and Downloading software

Because of the complex nature of the Facilities network and computing environment, staff should NOT install software themselves. Doing this, without proper testing, could cause a computer to stop functioning; or lead to loss of data and/or files.

Staff are asked to not download software (freeware, shareware, demonstrations) from the Internet; because of the risk of viruses and other malicious code being introduced on the network or workstation.

Staff should contact IT Services, who will download the software into a secure environment, test it for viruses and any compatibility problems, then make the application available for the user.

Please contact the IT Services staff if you have any questions; or would like to request software installations:

KATHI JESSE: 7-2899 KJesse@binghamton

JOE GOLDMAN: 7-4483 JGoldman@binghamton

1 March 2010

TO: All Physical Facilities staff

RE: Physical Facilities Color Printing policy

The use of color in business documents can be a significant help to the reader, when used appropriately. It is also important to control printing costs. Providing networked color printing resources allows all department staff to have access to this function; as well as better controlling the costs associated with color printing.

A. COLOR PRINTING AVAILABILITY:

Facilities computer users have access to 2 color printers that can be used by any department computer. These printers are connected on the network, and provide printing capability in a variety of paper sizes. Both printers are located in the Facilities building.

- HP DesignJet 4500 Plotter. This color plotter is used primarily for CAD and other large-scale work (sizes over 11"x17"). It prints on up to 36" wide paper. The plotter is not high-speed, and can't handle high-volume print jobs.

- HP LaserJet 5500 Color. This device is capable of very high-quality color printing; especially for photographs and other fine detailed jobs. It is high-speed, can take various paper sizes up to 11"x17", and can handle high-volume print jobs. Its use is closely monitored, and should only be used when high-quality color printing is an absolute necessity.

B. THE COST OF COLOR PRINTING:

Color printing is significantly higher in cost, when compared to monochrome printing. Color printing should be used only when absolutely necessary; not for routine print jobs. Monochrome printing is satisfactory for over 90% of the print jobs.

DeskJet printers (when compared to color LaserJets and monochrome printers) are slower, the amount of printed pages per cartridge is less, and replacement cartridges are more expensive.

Cost Comparison (Per Page)	**BLACK**	**COLOR**
LaserJet Printer (Color)	$ .02	$ .08
DeskJet/InkJet Printer	$ .04	$ .09
Copier Machine	$ .01	----

C. DEPARTMENT SUPPORT FOR COLOR DESKJET PRINTERS:

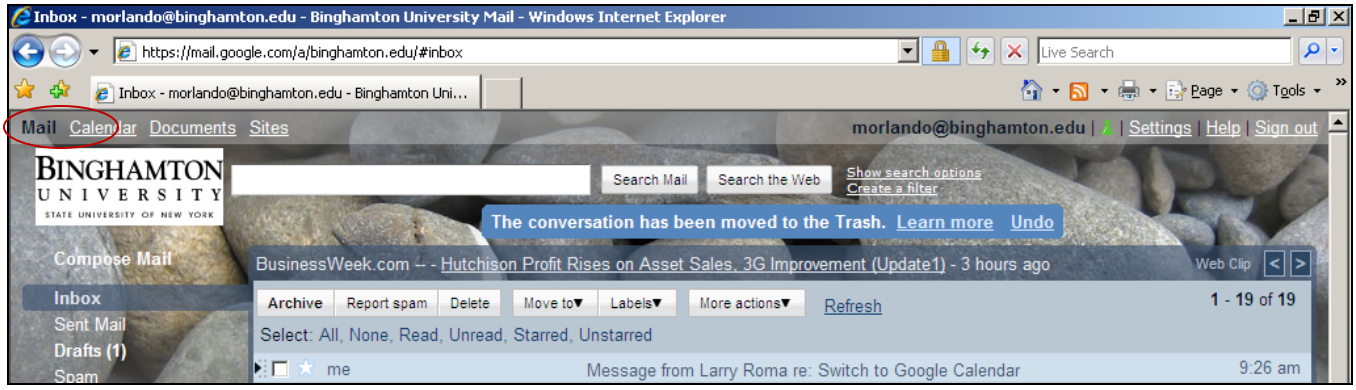
The department has a handful of smaller, color DeskJet printers that are used as local printers by some staff members; who are located in areas that don't have network printing available. Physical Facilities covers the cost of supplies for these "local printers" (including ink cartridges and paper).

These printers have become very expensive to support, due in large part to the rising costs of ink cartridges. Staff who have these DeskJet printers should make certain they use grey-scale for most print jobs. IT Services can assist with changing this setting.

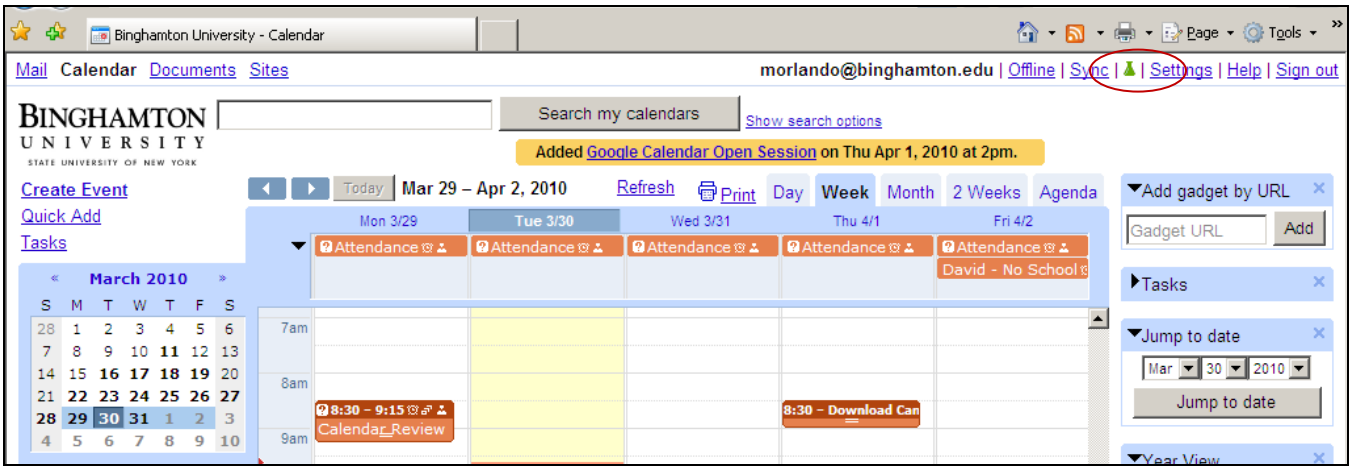
The department will provide one replacement color cartridge after the initial cartridge is expended. When the printer has to be replaced, a new monochrome LaserJet will be purchased to replace the DeskJet. If the staff member needs color printing – they will need to send their print jobs to one of the color printers on the network.

Setting Up Your Google Calendar

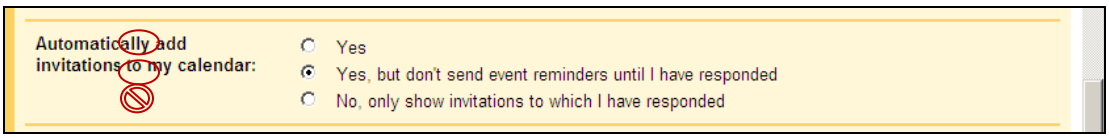
From your Bmail page, click on Calendar in upper left corner.



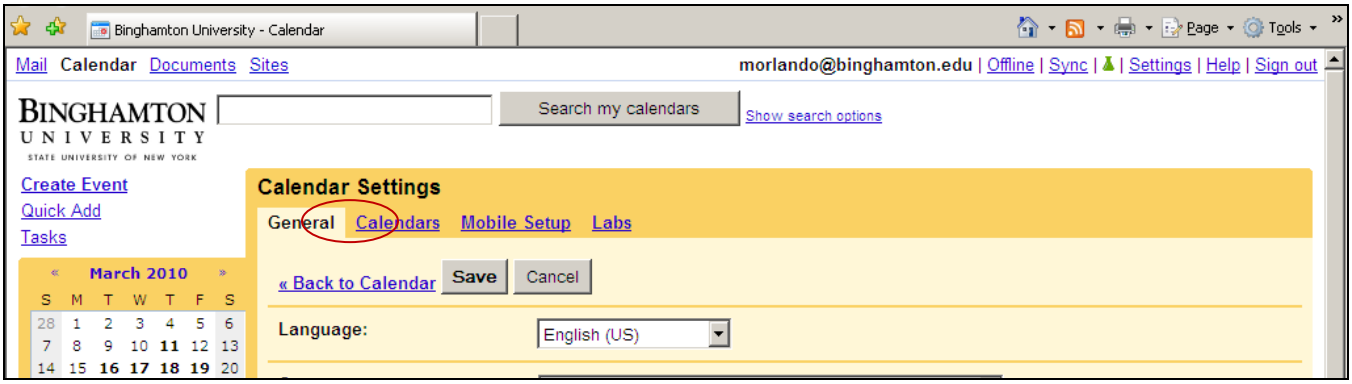
Your calendar will open in a new window. Click on Settings in upper right corner.



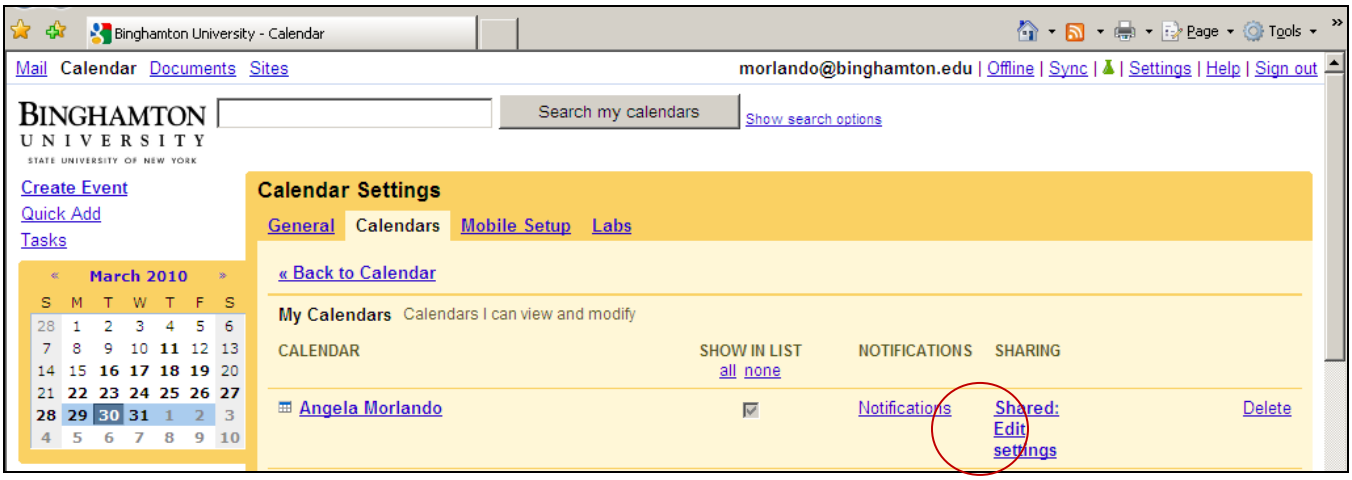
Scroll down and ensure that it is set to "Automatically add invitations" to your calendar. You may select "Yes" or "Yes, but don't send event reminders until I have responded". DO NOT select "No, only show invitations to which I have responded" as this could result in you being unaware of meetings to which you've been invited.



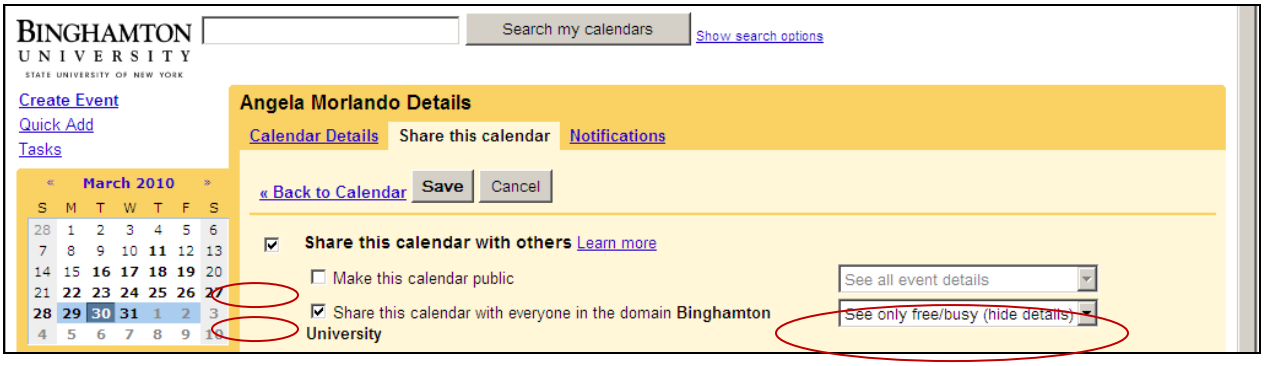
Scroll back to the top and click on the Calendars tab.



Under Sharing, click on Shared: Edit Settings (or Share this calendar)

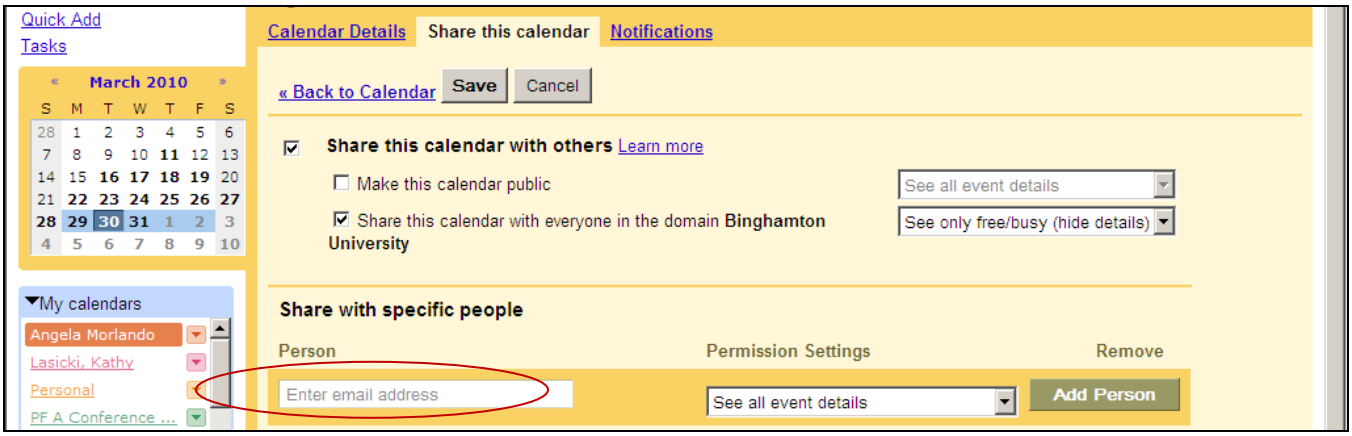


Verify that “Make this calendar public” is not checked and that “Share this calendar with everyone in the domain Binghamton University is checked with “See only free/busy (hide details)” in the drop-down box.



Under Share with specific people, give colleagues within your PF subunit(s) the ability to "See all event details" by individually typing their email addresses in the box.

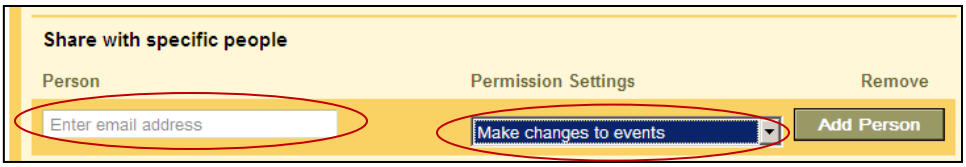
Administration	Business Affairs	Construction	Design	Long Term Planning	Operations	
Roma, Larry	Oaks, Sally	Markes, Robert	Muftic, Jesenko	Oaks, Sally	Kukawa, Mike	Custodial Days
Fennie, Karen	Ketchum, Jennifer	Lyon, Tom	Citriniti, Tony	McTiernan, Mary	Schneider, Wayne	Clark, Erika
Goldman, Joe	Berling, Juliet	Terzella, Chris	Hall, Bill	Afify, Mo	Allen, Mark	Jenkins, Bonnie
Kukawa, Mike	Brennan, Bonni		Sargent, Dell	Boston, Ken	Davis, Terry	Huyck, Sally
Markes, Bob	Cary, Diana		Barnum, Jim	Carruth, Mike	Price, John	Monaco, Silvana
Morlando, Angela	Curtis, Marty		Bourassa, Jennifer	Conklin, Nikki	Stone, David	Moore, Linda
Muftic, Jesenko	DeJohn, Sandy		Convertino, Jody	Jaycox, Rick		Morgan, Scott
Oaks, Sally	Ferraro, Johanne		Deeley, Paul	Konnick, Gregg	Crew Chiefs	Pflanz, Bob
	Ligas, Jay		Deskin, Michele	Langhans, Bob	Beach, Gary	Roys, Karen
	McCabe, Mike		Fletcher, Mary Ann	Whittemore, Don	Bundy, Dick	Vymislicky, Marlene
	McManus, Suzanne		Furch, Monika	Wilkins, Doug	Colwell, Mike	
	Shupa, Ray		Gilbert, Jason		Gowe, Steve	Custodial Nights
	Swift, Rose		Harrison, Ed		Kane, Kevin	Eaton, Joel
	Talcott, Rachel		Lewis, David		Lewis, Charlie	Bell, Rose Ann
	Williams, Mindy		Marr, George		Stein, Eric	Bruce, Todd
	Wolf, Amanda		Roglieri, Lyne		Towner, Nelson	Heatherman, Sharon
			Sklener, Lisa		Wilcox, Jerry	Hlavac, John
			Weeks, Heath		Ziac, Dave	Jackson, Robin
						Stephens, Sheila
					HVAC	
					Davis, Terry	CSC/Receiving
					Paffie, Chuck	Stone, David
					Williams, Rich	Contro, Diane
					Ziac, Dave	May, Joe
						Ostrander, Randy



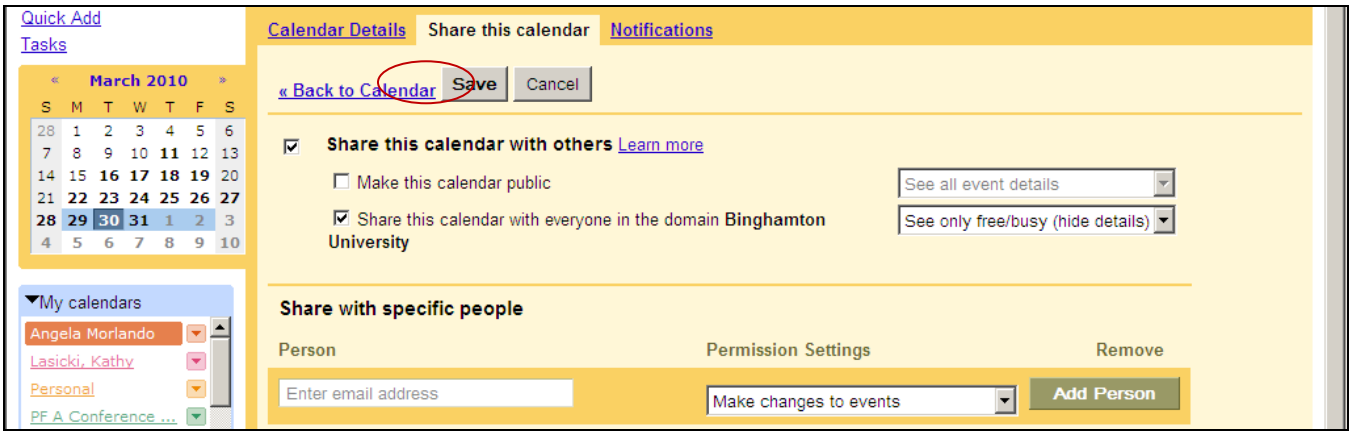
Change the drop-down box to "Make changes to events" and give **all** administrative support staff, not just your primary administrative assistant, permission to modify your events by individually typing their email addresses in the box.

Note: Anyone to whom you give permission to make changes to your events has access to ALL of your events, including those marked private. You should be mindful of this when scheduling events on your main calendar. You can create a secondary calendar (by clicking "Create new calendar" button under Settings – Calendars) which does not have to be shared for scheduling personal/confidential entries just be sure to block the time on your primary calendar as well to make yourself unavailable.

Administrative Support
Duff, Kristen
Lasicki, Kathy
Morlando, Angela
Nawrocki, Denise
Ostrander, Brenda
Reese, Hope
Ross, Fran
Terzella, Phyllis



Click Save at either the top or bottom of the screen.



You may wish to change your notifications settings that control when and how you are notified of changes to your calendar. This is also under Calendars in settings.