

## Terms of Service

### Syncing Personal Mobile Devices to Microsoft Exchange

Penn State Hershey enables access to the Microsoft Exchange system from the built-in email and calendar applications on personally-owned mobile devices. By opting in to this service, the authorized user trades some control over his/her personal device in exchange for access to Penn State Hershey resources (email). It is important that the consequences and obligations of this arrangement are well-understood. These obligations include, but are not limited to:

- User acceptance that a personal device may be reset to a factory default configuration (i.e., “wiped”, erasing all data and applications) remotely by Penn State Hershey, or automatically following a preconfigured number of failed attempts to access the device.
- User understanding that he or she is solely responsible for backing up any personal content on the device
- User agreement to keep the device updated and in good working order
- User acknowledgment that Penn State Hershey will in no way be responsible for damaged, lost or stolen personal devices while the user is performing organizational business
- User agreement to allow Penn State Hershey Information Technology (IT) to load manageability software on personally owned devices

## Scope

These Terms of Service apply to all users, (e.g., staff, faculty, students, contractors, consultants, and other authorized system users) worldwide who access and/or use Penn State Hershey’s Microsoft Exchange system from non-Penn State Hershey issued and owned devices.

## User Roles and Responsibilities

Despite individual ownership of the mobile device, the organization expects the user to assume certain responsibilities for any device that contains Penn State Hershey electronic information or connects to enterprise resources. Users must ensure that they comply with all sections of this agreement.

### Condition

- Users must maintain a device compatible with the organization's published technical specifications, which will be made available on the Penn State Hershey intranet. If a device falls out of compliance, then it may be blocked from access until it is in good working order and meets minimum requirements.

### Loss or Theft

- Users must report the temporary or permanent loss of personal devices immediately to the IT Technical Support Center by calling 717 531-6281 (to allow the device to be remotely wiped over the network) before cancelling any mobile operator services.

### Backup

- Users are responsible for backing up all personal information on their personal hard drives or other backup systems. Penn State Hershey cannot be held liable for erasing user content and applications when it is deemed necessary to protect enterprise information assets or if a wipe is accidentally conducted. Consult your device’s documentation for instructions on making secure backup copies.

## Functionality and Feature Management

- The device functionality must not be modified unless required or recommended by Penn State Hershey. The use of devices that are “jailbroken”, “rooted” or have been subjected to any other method of changing built-in protections is not permitted and constitutes a material breach of this policy.

- Users must accept that, when connecting the personal mobile device to Penn State Hershey resources, the Penn State Hershey security policy will be enforced on the device through technical controls. The security policy implemented may include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity, encryption, and automatically resetting to factory default configuration.
- Upon the organization's request, users must allow the installation of a mobile device management software agent, or any other software deemed necessary, on the user's device.
- Users must take appropriate precautions to prevent others from obtaining access to their mobile device(s). Users will be responsible for all transactions made with their credentials, and should not share individually assigned passwords, PINs or other credentials.

## **Failure to comply**

Violation of any provision of these terms or relevant Penn State Hershey policies may result in restriction or termination of a system user's access to Penn State Hershey/University Computer and Network Resources, including the summary suspension of such access and other disciplinary actions pursuant to applicable administrative, human resources and program specific policy. Further, such violation may subject you to civil or criminal penalties under federal, state or local laws.

## **Technical Support Processes**

### **How to Get Support**

The IT Technical Support Center will provide support for personal devices when it comes to connectivity and back-end system operational questions only. The IT Technical Support Center will not support device replacement, device upgrade, device operational questions or embedded software operational questions (such as questions related to the browser, email system, etc.). The IT Technical Support Center will only provide assistance on questions related to Penn State Hershey back-end software and the delivery of Penn State Hershey content to the device. All other inquiries must be directed to the end-user's mobile operator or other issuing retailer supporting the personal device.

### **Warranty and Replacement Responsibility**

If a user's device breaks or becomes damaged while conducting corporate business, Penn State Hershey will not reimburse the user for any repairs or replacements. Consult with your device's manufacturer or retailer for applicable warranty agreements or repair services.

## **Miscellaneous**

### **Discontinuation of Service**

When access to the Microsoft Exchange system is no longer authorized (due to separation from Penn State Hershey, suspension of service, or other reasons), users delete the Penn State Hershey account and all associated data from all mobile devices associated with this service. The Information Technology department may remotely wipe any such devices still accessing the Microsoft Exchange system after access to the service is no longer authorized.

### **Exceptions**

- Exceptions to these terms must be approved by the IT Director, Technical Services Engineering, the Chief Information Officer, or the Information Security Officer.

## Related Policies and Other Documents

HAM C-01	Confidentiality - Patient Information: Guidelines for Access, Use and Disposal
HAM C-03	Confidentiality - Electronic Communications and Messaging
HAM C-08	Confidentiality - Disposal of Information, Sanitizing of Electronic Media, and Destruction of Paper Documents
HAM C-18	Confidentiality - Appropriate Use of Electronic Information and Resources
HAM C-20	Confidentiality – Security Local and Remote Access and Use of PSH Electronic Information and Systems
HAM C-21	Confidentiality – Security Password Management
HAM C-37	Confidentiality – Security Electronic Storage of Sensitive Data
HAM C-42	Confidentiality- Reporting Suspected Breaches of PHI and Other Sensitive Data and Notification of Affected Individuals
PSU AD20	Computer and Network Security
PSU AD22	Health Insurance Portability and Accountability Act (HIPAA)
PSU AD23	Use of Intuitional Data

## Appendix A: Guidelines for Eligibility

Access to Penn State Hershey's Microsoft Exchange system is made generally available to all system users who agree to abide by the Terms of Service. This service should only be used where there is a justifiable business requirement for having mobile access to Penn State Hershey information.

Penn State Hershey reserves the right to deny eligibility for any reason, which may include working in a high-security area or department, working in a department with rigorous discovery and compliance requirements, users under a legal preservation order, temporary or probationary user status, or discontinuation of this service.

## Appendix B: Eligible Devices and Platforms

All devices connecting to the Penn State Hershey Microsoft Exchange system must support the technical policies outlined in Appendix C. These settings will be automatically set upon connecting to the Microsoft Exchange server, while non-compliant devices will be barred from connecting.

Information Technology will maintain minimum technical standards on the Penn State Hershey intranet. Devices falling outside these standard may be barred from connecting.

## Appendix C: Minimum Technical Security Requirements

All mobile devices connecting to Penn State Hershey's Microsoft Exchange system will be required to have the following security controls in place:

- The device must be protected by a 4-digit PIN or more complex password.
- The device must automatically lock after a maximum of 5 minutes of inactivity.
- The device must automatically be reset to a factory default state ("wipe", erasing all applications and data) after at most 10 consecutive failed attempts to unlock the device.
- The device must support IT or user initiated wipe through the Microsoft ActiveSync or BlackBerry Enterprise Server system console.
- The device must support automatically setting these controls through the Microsoft ActiveSync or BlackBerry Enterprise Server system console.