Washington University in St. Louis
INFORMATION SERVICES & TECHNOLOGY

- **Externally Hosted Computing Services Appropriate Use Guidelines**
- **Matrix for Appropriate Use**

Externally Hosted Computing Services
Appropriate Use Guidelines

This overview is intended to provide information for faculty, staff and students about the considerations and limitations for using the externally hosted computing services that have been arranged by university IT organizations. While there are examples of specific use cases and data types referenced in this summary, there may be data and concerns that are not addressed here. Technology capabilities and data communication needs are constantly evolving. When specific questions about the implications and risks of using an externally hosted service are not answered here, the individual user should consult with the IT organization that supports their area. The IT organizations will be responsible for publishing any specific guidelines for use of the technologies that they support.

The appropriate use of any technology assumes individual compliance with all university policies, legal and regulatory requirements, and funding agency requirements. The university's Code of Conduct specifies expectations for an employee's attention to policies and regulatory requirements. Loss or exposure of data that result from the inappropriate use of technology may be considered a violation of the university's information security or computer use polices, or other compliance requirements.

Background

IT leaders across the university, through the university's Technology Leadership Council (TLC), evaluate, select and acquire technology tools for use by the university community. Due diligence is performed to verify that tools and services provide appropriate levels of reliability, security, compatibility with our environments and compliance with legal and regulatory requirements. The Office of General Counsel, Resource Management and other organizations are engaged as appropriate to evaluate and negotiate terms and conditions. The Technology Leadership Council coordinates the adoption of technology services across schools to provide the most consistent and seamless services possible.

In general, the technology and services supported by the university's Information Services & Technology (IS&T) function and the school IT organizations are appropriate for use by faculty, staff and students for the conduct of the university's mission and administrative activities, with the exception of noted limitations or considerations as published in service descriptions or the appropriate use matrix.

The Appropriate Use Guidelines matrix (attached) provides an overview of common data storage and communication services, and considerations for use with different classifications of information. Questions about these services, or any not identified should be directed to your local IT support team. The information summarized in this document and the Appropriate Use Guidelines represents subsets of the types of data that are created, communicated and stored as part of university activities. These summaries are not all inclusive but do capture the most sensitive and regulated types of information. When communicating and storing university

information, it is always important to understand the type of information and to make appropriate arrangements to encrypt, use passwords, back-up or otherwise protect the information.

Externally Hosted Services

Several externally hosted or "cloud" technology solutions have been contracted for use by faculty, staff and students. These services have been evaluated and the terms and conditions for use reviewed to determine the capacity, limitations and appropriate uses of the solutions. The terms and conditions are for enterprise use and do offer greater protections than the consumer terms and conditions. The specific solutions that are currently available and a summary of the terms of use and any considerations for use are included in the attached Hosted Service Profiles.

While IS&T and IT leadership within schools are confident that the tools procured and the services arranged meet the university's standards for reliability, security, compatibility and compliance, all risk of a service failure or data exposure for either internally or externally managed services cannot be eliminated. When used in accordance with security policies, guidelines for handling of sensitive data, and the considerations noted in the Hosted Service Profiles, the IT support commitment and employee risks from use of the external services will be the same as for an internally provided service.

Washington University in St. Louis
INFORMATION SERVICES & TECHNOLOGY

Hosted Service Profile: Office 365

Vendor: Microsoft

Office 365 Email and Calendar are core services within the Microsoft hosted software provided to eligible members of the university community including the CFU, Danforth Campus schools and students. The School of Medicine has not identified Office 365 as appropriate for use and continues to manage an internally hosted email and calendaring service.

Summary of Terms and Conditions

- Data ownership – The ownership for all email, attachments and documents stored in the Microsoft environment is the same as in an internally hosted environment. WUSTL has the ability to access and retrieve data to support normal business operations, respond to legal requests, and to recover data and services.
- Data access and use by the vendor – Microsoft may only access WUSTL data stored in their environment for the purpose of maintaining the service, responding to valid legal requests or for resolving security threats. Microsoft will not access WUSTL data for the purpose of marketing, analysis of user behavior or for purposes not related to providing email, file storage and web conferencing services.
- Data back-up and recovery – Data is retained until deleted by the end user or termination of the service by WUSTL. In the event the service is terminated, WUSTL will work with Microsoft to copy email, calendars and files to a university service or to a replacement third party service.
- Security – All data associated with these services will be housed in multiple Microsoft owned geographically separated, enterprise-grade data centers within the United States. Microsoft commits to maintaining security in compliance with the ISO/IEC 27000 series of standards. This compliance is audited annually and WUSTL has the right to access the results of the audits.
- FERPA – Microsoft agrees to comply with FERPA regulations.
- HIPAA – There is a HIPAA Business Associates Agreement in place between WUSTL and Microsoft.

Considerations for Use

Office 365 Email and Calendar are covered by the university's agreements with Microsoft. These services provide secure environments for maintaining or sharing the university's sensitive unregulated data, as well as some kinds of sensitive regulated data.

WUSTL IT leadership has determined that hosted Microsoft Office365 is a reliable, secure and credible service. When used in compliance with university policies for information security, computer use and the code of conduct, the hosted services should be considered an extension of internally provided services.

The use of email for communication of any sensitive information is generally discouraged and is sometimes prohibited, whether the email service is supported inside or outside the university. Files with sensitive information that are attached to emails or posted in any shared workspaces should be properly encrypted and/or password protected.

Social Security Numbers or other personal identity information (PII) should only be used where required by law or where it is essential for university business processes. IS&T can help you explore appropriate ways to encrypt, securely transmit or store SSNs and PII when there is a legitimate business reason.

Office 365 Email and Calendar **may not** be used for

- Payment Card Industry (PCI) information
- Export Controlled Research (regulated by ITAR or EAR)

These data restrictions are compliance-based, not security-based. Regulatory requirements mandate that specific sensitive regulated data be restricted from this service. Office 365 may not be used for Export Controlled Research data because Microsoft cannot ensure that only U.S. persons have access to or maintain its systems.

Appropriate Data Use

✓	Appropriate
X	Not Appropriate
?	Appropriate with assistance from IS&T or school IT organization

- ✓ Attorney/Client Privileged Information
- ✓ IT Security Information
- ✓ Other University Sensitive Data not explicitly addressed elsewhere
- ✓ Student Education Records—FERPA
- ✓ Student Loan Application Information—GLBA

- ? Social Security Numbers
- ? Personally Identifiable Information (PII)
- ? Federal Information Security Management Act (FISMA) Data
- ? Protected Health Information—HIPAA
- ? Sensitive Identifiable Human Subject Research

- X Credit Card or Payment Card Industry (PCI) Information

- X Export Controlled Research—ITAR or EAR

Hosted Service Profile: Box

Vendor: Box.net, Internet2

Box is a cloud-based storage solution that allows you to share files with people inside and outside of the university. Internet2 and Box.net have partnered to work with representative universities to develop a hosted service that meets common higher education security and regulatory requirements.

Summary of Terms and Conditions

- Data ownership – The ownership for all documents stored in the Box environment is the same as in an internally hosted environment. WUSTL has the ability to access and retrieve data to support normal business operations, respond to legal requests, and to recover data and services.
- Data access and use by the vendor – When you upload a file to Box, it is **private by default and encrypted when stored**. Your files are only accessible to others if you share them or make them public. Box may only access WUSTL data stored in their environment for the purpose of maintaining the service, responding to valid legal requests or for resolving security threats. Box.net will not access WUSTL data for the purpose of marketing, analysis of user behavior or for purposes not related to providing file storage services.
- Data back-up and recovery - Box stores local snapshots of data and backs up all data daily to a facility in a separate location. Data is retained until deleted by the end user or the agreement with WUSTL is terminated. In the event the agreement with Box is terminated, WUSTL will coordinate transferring data from Box to another service.
- Security – Box hosts its servers at **multiple geographically separated, enterprise-grade data centers** in the United States with a 99.9% network uptime guarantee, SSAE 16 Type II security standards, ongoing audits and 24x7x365 monitoring and video surveillance. Data is stored on a secure internal storage cluster behind an enterprise-grade firewall, with redundant connections to multiple Internet backbones. The software passes every request through a carefully audited verification code, which ensures that the user is authorized for the action requested. All user data is stored in encrypted form. Keys are held by Box under strictest security. 256-bit Secured Socket Layer (SSL) encryption is used on the data between the end user and Box.
- FERPA – Box agrees to comply with FERPA regulations.
- HIPAA – There is a HIPAA Business Associate Agreement in place between WUSTL and Box.

Considerations for Use

Box is a contracted-for service obtained through a partnership with a consortium of higher education institutions. The agreement includes confidentiality and data security provisions. Box provides a secure environment in which to maintain or share the university's sensitive unregulated data, as well as some kinds of sensitive regulated data. WUSTL IT leadership has determined that hosted Box is a reliable, secure and credible service. When used in compliance with university policies for information security, computer use and the code of conduct, and subject to the considerations in this document, the hosted services should be considered an extension of internally provided services.

Social Security Numbers and other personal identify information should only be used where required by law or where they are essential for university business processes. If you must use SSNs, it is preferred that you use institutional resources designed to house this data. IS&T can help you explore appropriate storage locations or work with you to appropriately encrypt the data if those alternatives will not work for you.

These Box.net applications **may not** be used for Export Controlled Research because Box cannot ensure that only U.S. persons have access to or maintain their systems. Data will be stored in U.S. based data centers only and all data is stored in an encrypted form.

We believe that Box is **compliant with most grants**, although specific grant rules for data management should be checked prior to use for research data.

A detailed description of the Box service features can be found at
http://www.internet2.edu/netplus/box/faq.html

Appropriate Data Use

✓	Appropriate
X	Not Appropriate
?	Appropriate with assistance from IS&T or school IT organization

- ✓ Attorney/Client Privileged Information
- ✓ IT Security Information
- ✓ Other University Sensitive Data not specifically addressed elsewhere
- ✓ Sensitive Identifiable Human Subject Research
- ✓ Student Education Records—FERPA
- ✓ Student Loan Application Information—GLBA

- ? Protected Health Information—HIPAA
- ? Social Security Numbers
- ? Personally Identifiable Information (PII)
- ? Federal Information Security Management Act (FISMA) Data

- X Credit Card or Payment Card Industry (PCI) Information
- X Export Controlled Research—ITAR or EAR

Data Storage and Transport Services
Appropriate Use Guidelines

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

Appropriate | Not Appropriate | Appropriate with help from IS&T or school IT leadership

Attorney Client Privileged	Confidential	Confidential communications between a client and an attorney for the purpose of securing legal advice.	Communications related to a lawsuit. Communications related to a contract, such as email between the WUSTL Office of the General Counsel and Procurement Services related to a contract dispute with a vendor.								NA			
Credit Card or Personal Credit Information - PCI	Protected	Information related to credit, debit, or other payment cards. This data type is governed by the Payment Card Industry (PCI) Data Security Standards and overseen by the WUSTL Cash and Credit Operations Office. Credit or debit card numbers cannot be stored in any electronic format without the expressed, written consent of the WUSTL Cash and Credit Operations Office. That office is responsible for the only PCI-compliant environment at the university.	Cardholder name Credit/debit card account number Credit/debit card expiration date Credit/debit card verification number Credit/debit card security code											
Social Security Numbers	Confidential	Social Security Numbers are unique, nine-digit numbers issued to U.S. citizens, permanent residents, and temporary (working) residents for taxation, social benefits, and other purposes.	Numbers in this format: 123-45-6789 that uniquely identify an individual for tax purposes											
Personally Identifiable Information (PII)	Confidential	Personally Indentifiable Information (PII) is a category of sensitive information that is associated with an individual person, such as an employee, student, or donor. PII should be accessed only on a strict need-to-know basis and handled with care. PII is information that can be used to uniquely identify, contact, or locate a single person. Personal information that is “de-identified” (maintained in a way that does not allow association with a specific person) is not considered sensitive.	**For Everyone at WUSTL:** Social Security number National ID number Passport number Visa permit number Driver's license number Bank and credit/debit card numbers Tax information (e.g., W-2, W-4, 1099) Disability information Ethnicity Gender **For Employees:** Date and location of birth Country of citizenship Citizenship status Marital status Military status Criminal record Home address											

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

Appropriate

Not Appropriate

Appropriate with help from IS&T or school IT leadership

Grievance information
Discipline information
Leave-of-absence reason
Benefit information
Health information

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

Appropriate | Not Appropriate | Appropriate with help from IS&T or school IT leadership

			For Students: Wire transfer information Student tuition bills											
Student Education Records - FERPA	Protected	Records that contain information directly related to a student and that are maintained by WUSTL or by a person acting for the university. The Family Educational Rights and Privacy Act (FERPA) governs release of, and access to, student education records. Directory information about a student is not regulated by FERPA and can be released by the university without the student's permission. Students can request non-disclosure from the WUSTL Registrar's Office.	Student transcripts and grades Degree information Class schedule Advising records Disciplinary records Other non-directory information Athletics or department recruiting information								NA			
Student Loan Application Data - GLBA	Protected	Personal financial information held by financial institutions and higher education organizations as related to student loan and financial aid applications. Gramm Leach Billey Act (GLBA) provisions govern this data type.	Student loan information Student financial aid and grant information Payment history											
Protected Health Information - HIPAA	Protected	Protected Health Information (PHI) is any health information that can be linked to an identifiable individual, such as a patient receiving treatment at a WUSTL or BJC facility. PHI is regulated by the Health Insurance Portability and Accountability Act (HIPAA). Researchers should be aware that health and medical information about research subjects may also be regulated by HIPAA. Researchers should contact the WU School of Medicine Compliance Office with questions.	The following individually identifiable data elements, when combined with health information about that person, make such information protected health information (PHI): Names Telephone numbers Fax numbers Email addresses Social Security Numbers Medical record numbers Health plan beneficiary numbers License plate numbers URLs Full-face photographic images Any other unique identifying number, characteristic, code, or combination that allows identification of an individual								NA			

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites
Sensitive Identifiable Human Subject Research	Protected	Individually identifiable research data containing sensitive information about human subjects. A human subject is a living individual about whom a researcher obtains data and information that can be used to identify him or her.	Sensitive identifiable information may include research data referring to: Illegal behaviors Drug or alcohol abuse Sexual behavior Mental health or other sensitive health or genetic information Any data collected under a National Institutes of Health (NIH) Certificate of Confidentiality is considered sensitive.								NA			
Grant Applications	Confidential	Grant proposal development and applications may contain information that describes unique or differentiating concepts, ideas or processes. Exposure of this information may negatively impact opportunities for grant funding.	Research protocols Research hypotheses								NA			
Export Controlled Research - ITAR, EAR	Protected	Export Controlled Research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism, or non-proliferation. The International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) govern this data type. Current law requires that this data be stored in the U.S and that only authorized U.S. persons be allowed access to it.	Chemical and biological agents Scientific satellite information Certain software or technical data Military electronics Nuclear physics information Documents detailing work on new formulas for explosives								NA			
Federal Information Security Management Act - FISMA	Protected	The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document, and implement security programs for IT systems and store the data on U.S. soil. FISMA applies generally to federal contracts as opposed to grants.	Data provided by the federal government under contract								NA			
IT Security Data	Confidential	IT Security Information consists of information that is generated as a result of automated or manual processes that are intended to safeguard the university's IT resources. It includes settings, configurations, reports, log data, and other information that supports IT security operations.	IT security program plans IT security incident information Access and authentication logs Firewall rules								NA			
University Correspondence	Confidential	Information that could be embarassing or damaging to individual or university reputations may be contained in correspondences or notes of meetings and conversations. University correspondence, Board and committee meeting minutes, presentation materials, and other documents that capture internal communication should be treated as sensitive.	Admissions and recruiting correspondence Search committee correspondence, minutes and notes Personnel evaluations Employment applications								NA			

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

Appropriate | Not Appropriate | Appropriate with help from IS&T or school IT leadership

Data Storage and Transport Services
Appropriate Use Guidelines

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites
			Board of Trustee or National Council correspondence											

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

Appropriate

Not Appropriate

Appropriate with help from IS&T or school IT leadership

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

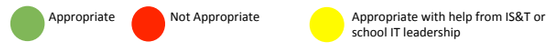
Appropriate | Not Appropriate | Appropriate with help from IS&T or school IT leadership

Other University Sensitive Data	Confidential	According to university policy, data will typically be classified as sensitive if any of the following are true: Unauthorized disclosure may have serious adverse effects on the university's reputation, resources, or services or on individuals It is protected under federal or state regulations. There are proprietary, ethical, or privacy considerations.	Due to the nature of the definition of sensitive data, it is impossible to have an exhaustive list of sensitive data examples. While the most common types of sensitive data are already included in this guide, there are many other examples of sensitive data, including: Public safety information Certain types of information about hazardous substances Proprietary information such as computer source code developed at the university Information about misconduct proceedings	Yellow	Green	Green	Green	Green	Yellow	Green	NA	Red	Red	Red

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation



(1) Information Classification

Public
Public Information consists of information that is acceptable to share openly and has no requirements from federal or local regulations on its control and use.

Confidential
This classification is to be used for information that is not freely available to use, store, and transmit. Some types of confidential information may be subjet to regulatory or legal rules. Items considered intellectual property of a research group or business unit, employee salaries, human resource files and legal documents would fall into this category. This information is for limited distribution and requires basic information security controls.

Protected
Information that has specific requirements for controls on its use, storage and transmission as mandated by federal, state and local regulations is considered "protected" information. Regulations including but not limited to:

- Health Insurance Portability and Accountability (HIPAA) covering protected health information
- Federal Information Security Management Act (FISMA) when creating, storing information for federal agencies.
- Payment Card Industry (PCI) Data Security Standards (DSS)
- Department of Homeland Security (DHS) covering controlled chemicals and substances

(2) University or School Managed Services

Email
This includes email storage and transporation systems hosted on university premises and managed by university personnel. The most common services at WUSTL are Microsoft Exchange and LINUX native services. Email clients that replicate university email to a local device should be limited to operation on a device that is secured with a password and/or encryption. When accessing email remotely via a web client, precautions should be taken to fully sign-off of the web session and close the browser.

Secure FTP
Many department and school IT organizations support secure FTP services. Contact your IT support resource for information. Not all FTP services are appropriate for protected health information. Contact the School of Medicine Information Security Office before using FTP to transfer HIPAA regulated information.

File Storage
File and print servers are provided by most campus IT organizations as a way to store individual's files in high capacity, secure environments with regular data back-up. These file servers reside within a school or university network.

File Sharing
Two options for sharing large files among multiple WUSTL employees and students are hosted within the university's environments. Both options require a valid WUSTL key for access.
WUSTL Dropbox (https://dropbox.wustl.edu)
WUSTL Large File Transfer System (https://lft.wustl.edu)

Transaction Systems
Systems that are developed or purchased to support daily processes and transaction mangement. Examples include but are not limited to the following:

Information	Classification (1)	Definition	Examples	University or School Managed Service (2)					Externally Hosted Services with University Contract (3)			Personally Arranged Services (4)		
				Email storage & transport	Secure FTP	Managed File Storage	File sharing services	Trans-action Systems	Office 365	Box.net	Cashnet	Email (Gmail, Hotmail, Yahoo, etc.)	Dropbox.com	Websites

The information summarized below represents subsets of the kinds of information that is created, communicated and stored as part of university activities. This information summary is not all inclusive but does capture the most sensitive and regulated types of information. When communicating and storing university information , it is always important to understand the type of informationand to make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.

Appropriate Use Designation

Appropriate | Not Appropriate | Appropriate with help from IS&T or school IT leadership

Financial Information System (FIS)

Student Information System (SIS)

Student Financial System (SFS)

Blackboard Learning Management System (LMS)

Undergraduate Admissions (UA)

Alumni & Development Information System (ADIS)

Human Resources Management System (HRMS)

Proposal Development System (PDS)

Sponsored Projects Accounting (SPA)

Physicians Billing

WUSTL Connect/Key

(3) Externally Hosted Services with a University Contract

Office 365 Email
Office 365 Email and Calendar are core services within the Microsoft hosted software provided to eligible members of the university community including the CFU, Danforth Campus schools and students. The School of Medicine has not identified Office 365 as appropriate for use and continues to manage an internally hosted email and calendaring service.

Box.net
Box is a cloud-based storage solution that allows you to share files with people inside and outside of the university. There are many applications that can be used within Box. WUSTL users can use any of those applications, but only the Core Applications have been tested and approved by WUSTL.

Cashnet
Cashnet is a third-party service for processing credit card transactions that is fully PCI compliant when used in coordination with the WUSTL Cash and Credit office and IS&T. There are requirements for encryption of data collection and transmission that must be followed in order to remain PCI compliant.

(4) Personally arranged consumer services

The use of consumer services for email, file storage or website support for university activities is generally discouraged. The terms for individual use of consumer tools may not provide the same level of security and compliance assurances that have been defined in university agreements. Examples of the use of personally arranged consumer services include forwarding university email to personal Gmail, Hotmail or Yahoo email accounts. Decisions to assume the potential risks of using these services for university data and business are the responsibility of each individual. It is important in all cases to understand the type of information being communicated or stored and make the appropriate arrangments to encrypt, use passwords, back-up or otherwise protect the information.