Members:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raina Bloom</td>
<td>AS</td>
<td>School of Information Studies</td>
</tr>
<tr>
<td>John Jordan</td>
<td>FAC</td>
<td>Communication</td>
</tr>
<tr>
<td>Ed Mabry</td>
<td>FAC</td>
<td>Communication</td>
</tr>
<tr>
<td>Ethan Munson</td>
<td>FAC</td>
<td>Elec Engineering &amp; Comp Sci</td>
</tr>
<tr>
<td>Christopher Burns, Chair</td>
<td>FAC</td>
<td>Music</td>
</tr>
<tr>
<td>Prasenjit Guptasarma</td>
<td>FAC</td>
<td>Physics</td>
</tr>
<tr>
<td>Stephen Pevnick</td>
<td>FAC</td>
<td>Art &amp; Design</td>
</tr>
<tr>
<td>Brad Houston</td>
<td>AS</td>
<td>Libraries</td>
</tr>
<tr>
<td>Chiu Law</td>
<td>FAC</td>
<td>Elec Engineering &amp; Comp Sci</td>
</tr>
<tr>
<td>Michael Zimmer</td>
<td>FAC</td>
<td>School of Information Studies</td>
</tr>
<tr>
<td>Tracy Buss</td>
<td>AS</td>
<td>International Education Ctr</td>
</tr>
<tr>
<td>Woonsup Choi</td>
<td>FAC</td>
<td>Geography</td>
</tr>
<tr>
<td>Kristene Surerus</td>
<td>FAC</td>
<td>Chemistry</td>
</tr>
<tr>
<td>Bo Zhang</td>
<td>FAC</td>
<td>Educational Psychology</td>
</tr>
<tr>
<td>Sandra Braman</td>
<td>FAC</td>
<td>Communication</td>
</tr>
<tr>
<td>John McCarragher</td>
<td>In Dir</td>
<td>UITS</td>
</tr>
<tr>
<td>Laura Pedrick</td>
<td>AS</td>
<td>Provost Designee</td>
</tr>
<tr>
<td>Daniel Laughland</td>
<td>Student</td>
<td></td>
</tr>
</tbody>
</table>

Charter:
Functions/ Responsibilities:

A3.2 Information Technology Policy Committee

(1) Membership. Eighteen members as follows: eight elected faculty; two from each division of the University, elected by division; four appointed faculty, one from each division appointed by the Chancellor from nominations submitted by the University Committee; three elected members of the academic staff, with at least one representing full-time teaching staff; one student; and, ex-officio, the Director of Information and Media Technologies, and a representative of the Provost.

(2) Functions.
Makes recommendations to the faculty and campus administration regarding (a) policy or information technology and its use; (b) the coordination of service delivery by all campus
information technology units, including monitoring, overlap, conflicts and inefficiencies; and (c) the implementation of decisions pertaining to information technology and related services.

(Document 2265, 11/16/00; UWM Administration approval, 12/1/00)
(Editorially revised, 4/26/02)

Meetings:

The ITPC met seven times: September 9, October 14, November 4, and December 2, 2011, and March 2, April 6, and May 4, 2012.

The committee:

1. Passed a resolution (attached) advocating significant upgrades to UWM's core network infrastructure, to address ongoing issues with our wired and wireless networks. Campus administration has announced that we will be moving forward with these improvements, and the procurement, installation, and configuration of necessary equipment is now underway.

2. Discussed at length the reorganization of IT services at UWM announced by campus administration in November. A subcommittee of ITPC members met with the Chancellor, Provost, Vice-Chancellors Brown and Luljak, and CIO McCarragher to discuss coordination and implementation issues raised by the reorganization; Provost Britz met with the committee to discuss this issue in December 2011 and May 2012, and Vice-Chancellor Luljak also attended the May 2012 meeting.

3. Heard a briefing from Vice Chancellor Tom Luljak, Steve Brukbacher (UITS Security), and Paul Rediske (Internal Audit) regarding the Summer 2011 security incident, disclosure to individuals whose personal information may have been compromised, and post-incident audit and review of security procedures.

4. Discussed the "Future of Email/Calendaring" working group report, and the Provost's decision to move forward with a Request for Proposals for a third-party, cloud-based email service to replace the existing Pantherlink system. The report suggests that this move will provide the campus with new capabilities, improve reliability, and reduce costs, and that concerns about privacy, offshore transfer of intellectual property, and etc. can be mitigated through negotiations with the service providers.

5. Discussed and endorsed guidelines (attached) for the digitization of paper records by campus units, and discussed guidelines for the archiving of faculty electronic records which fall under the purview of state records retention law.

6. Discussed continuing campus needs surrounding research computing.

7. Heard briefings from UITS staff regarding changes in Pantherlink email quotas, the operation and utilization of the Avi high-performance computing cluster shared by CEAS, L&S, and Freshwater Sciences, the current status of UWM's core network, implementation of the pilot UWM Wifi project, plans to expand the rollout of the UWM Wifi service,
continuing development of mobile applications, and the formation of a Content Management System Advisory Board.

8. Heard briefings from Academic Affairs staff regarding upcoming phases of the Digital Future initiative, and regarding the Educational Technology Fund process for this year.

9. Elected Professor Ethan Munson (Computer Science) as chair of the committee for 2012-2013.
Prioritizing the upgrade and renewal of UWM's information technology infrastructure
approved by the Information Technology Policy Committee, 2011.12.02

The aging of UWM's core network, and the absence of adequate recurring resources for its renewal, represent a looming crisis. Our technological infrastructure is obsolete, fragile, over capacity, and incapable of meeting modern security standards. An outdated network design and obsolete equipment are being stressed by radically increased demands for network bandwidth. Catastrophic failure is increasingly likely, and places the entire university's mission is at risk.

Information technology infrastructure underlies the work of every aspect of the university: teaching and learning, research, and administration all depend upon the stable functioning of networked systems and services. Over the past twenty years, the network has silently and gradually become a critical strategic element of UWM's core mission. However, the personnel and resources devoted to infrastructure maintenance and renewal have not reflected that transformation. We recognize that the rapid pace of change in the IT field makes it particularly challenging to address, and that the renewal of our technological infrastructure is one of many worthy initiatives clamoring for attention in an era of scarce resources. However, the updating of the core network needs to become an immediate priority.

There are substantial risks and costs associated with delay or failure to resolve this issue. Faculty are reporting the disruption of lesson plans due to Prowlnet outages. The university's extramural research funding is threatened by our network's incompatibility with HIPAA security standards. Our ability to recruit faculty, staff, and students is diminished when we fail to meet the contemporary expectation of ubiquitous wireless networking. Network outages are a campus climate issue, interrupting work across the university, and causing significant frustration. There is also significant risk of an extended outage, which would damage the university's reputation, cost enormous amounts in lost work, and drive up the expense of upgrade and renewal by treating it as repair and mitigation.

A number of specific actions, all of which are interconnected, are needed:

- **Extend the UWM WiFi service across campus and decommission Prowlnet**

  The campus wireless network is the highest-profile source of outages at present. The Prowlnet network, originally intended to provide limited "hotspots" on campus, has been stretched by its extension to near-ubiquitous service across the campus. At the same time, it is being deluged by the exponentially increasing number of wireless devices at UWM. At times of peak usage, Prowlnet is seeing requests from 3,000 devices above its capacity; the security controllers in particular are being overwhelmed by the number of devices. We anticipate that the number of devices being brought to campus will make another significant jump after the coming holiday gift-giving season, increasing the severity of this issue.

  The pilot UWM WiFi service, funded through student EdTech fees, has the potential to offer significant improvements (it implements the current 802.11n standards for higher bandwidth and capacity, and supports encryption as well as superior authentication). However, funding support is needed to extend the service beyond the Union and Golda Meir Library and across the campus as a whole.
• Replace the routers comprising the core network

The effective functioning of the UWM WiFi wireless service depends in turn upon our aging and insufficient wired network. The four routers which comprise the core of our network all include components which are “End of Support” (EOS), meaning that the vendor is no longer supplying maintenance updates, bug fixes, or security patches. Additionally, two of the four router chassis will be EOS on November 1, 2012, and none of the routers are adequately provisioned with “failover” components that will ensure graceful continuation of network routing in the case of a hardware fault.

• Upgrade the ring network to provide redundancy in case of a core network failure

The ring of devices around the core routers should be capable of carrying network traffic in the event of a core failure. However, UWM’s ring will not in practice provide this redundancy; the ring switches are not capable of routing traffic, and the network bandwidth is not high enough to handle the load.

• Replace obsolete equipment outside of the core and ring networks

The switches which connect the ring network to individual campus buildings have all been EOS since September 17, 2010.

In addition to these critical fixes, UWM needs to adopt a more proactive stance towards the maintenance and renewal of its IT infrastructure:

• Plan for the upgrade and renewal of campus fiber

Below the level of routing and switching, campus fiber links (installed in 1990) are nearing maximum capacity.

• Provide recurring resources for the ongoing maintenance and renewal of infrastructure

The replacement of critical equipment must be backed by a plan for regular maintenance and upgrades. Short-term solutions without long-term planning will lead us back to our current situation.

• Ensure that there are adequate personnel to execute these plans

The personnel for testing, implementation, operation, and maintainence are a critical part of the equation for a smoothly functioning infrastructure.

There is broad campus support for a resolution to the issues facing our information technology infrastructure. Repeated ITPC (November 2007 and December 2010) and Senate resolutions (Faculty Document 2768, February 2011) address this question. All three of the surveys (teaching/learning, research, and administration) associated with the Digital Future report ranked infrastructure as a high priority.
Networking and infrastructure underlie all of the goals and objectives which have been highlighted by the Digital Future report. The Digital Future initiative is a once-in-a-generation opportunity for UWM to establish a campus identity around the effective and innovative deployment of technology in higher education. As part of that process, we urge campus leadership to move as rapidly as possible to upgrade our core IT infrastructure, and to establish appropriate recurring resources for its maintenance and renewal.
Digitization of Departmental Records

Digitization, or digital imaging, is an increasingly popular strategy for departments and offices looking to manage their records. When implemented appropriately, digitization can dramatically improve access to records while simultaneously reducing the need for physical records storage space. However, digitized records introduce new responsibilities, costs, and challenges not present in management of paper records. These guidelines are intended to help UWM departments determine if digitization of their records is an appropriate course of action, and if so to assist them in developing a secure and robust digital imaging program and associated processes.

NEEDS ASSESSMENT AND COST ANALYSIS

Before embarking on a digitization program, departments should assess whether digitization is an appropriate solution for their records management needs. In general, digitization is best implemented in cases where quick, simultaneous, and/or distributed access to records is necessary for fulfillment of a department’s responsibilities, or when such access would significantly increase the efficiency of a department’s operations. Digitization is generally NOT an appropriate solution for reducing storage costs, as the cost of hardware, software, storage space, training, and maintenance of systems can greatly exceed the cost for storing those same records in paper form.

Some of the factors that must be evaluated during an initial needs assessment include:

- **Program Purpose:** Why is the digitization program being undertaken? Will digitized records be maintained in lieu of or in addition to paper records?
- **Business Process Evaluation:** how does the digitization program improve business processes?
- **Information Security:** What security precautions must be taken to protect digitized records?
- **Amount and Accumulation:** How many records are to be digitized? What is the estimated rate of addition per year to these records?
- **Type of Record:** What type of document (textual, photograph, map, etc.) is to be digitized? How does that affect the need to provide additional information about the records?
- **Records Retention:** How long must digitized records be retained? Are the records scheduled under a current Wisconsin Records Retention and Disposition Authority (RRDA)?

For a cost analysis, some of the factors to consider include:

- e) **System Hardware and Software**
- d) **Image Management Application**
- e) **Facilities Upgrades/Site Preparation** (including additional storage space)
- f) **Project Management**
- g) **Training**
- h) **Staffing**
- i) **Ongoing Maintenance, Support, and Upgrade** (generally about 10-20% annually of initial implementation cost)

If a cost analysis does not yield a net benefit for a digitization program, consider retaining files in paper form in your office, or explore storage alternatives (off-site storage, etc.).
See also UWM Records Management Guideline #2, Offsite Records Storage: http://www4.uwm.edu/libraries/arch/recordsmgt/guideline2offsite.cfm

SYSTEM SPECIFICATIONS AND SELECTION
Due to the broad scope of most digitization projects, departments are strongly encouraged to select a reliable vendor for scanning of records and management of digitization systems. This selection should be pursued through UWM’s normal procurement channels in consultation with Purchasing and UITS, as detailed at http://www4.uwm.edu/bfs/procedures/purch/. RFPs for Digital Imaging Systems should include, at minimum, the following requirements:

- **Open systems architecture**, including non-proprietary compression standards. This type of architecture allows the system to be upgraded over time without a significant risk of records loss. It also supports the importing and exporting of digital images to and from other sources. If proprietary standards or architecture are unavoidable, the vendor should provide a bridge to systems with non-proprietary configurations and/or license the software beyond the length of the contract.

- **Specifications for hardware/software that will require vendors to support and maintain their product(s).**

- **Controls and system auditing tools.** Effective audit trails can automatically detect who had access to the system, whether staff followed existing procedures, or whether fraud or unauthorized acts occurred or are suspected.

- **Image authenticity/integrity tools.** The system should ensure that the images are protected from accidental or intentional modification. Equipment should also conform to methodology for media error detection and correction.

- **Records management system integration.** System records should be linked to approved RRDAs and retention periods and include provisions for automatically or manually purging records beyond their scheduled retention dates. See Records Management, below.

- **Appropriate document scanning resolution.** Consider data storage requirements, document scanning rates, and the accurate reproduction of the image. See Technical Specifications, below.

- **Access to records.** Systems should use an indexing system database that provides for efficient retrieval, ease of use, and up-to-date information on the scanned images stored in the system. The index storage method should be based on standard relational database technologies with access using standard SQL queries. See Metadata Integration, below.

- **Appropriate levels of security.** Systems should ensure that only authorized personnel are able to create, copy, modify, or use scanned images within the system. Different types of scanned records may include different security requirements. See Information Security, below.

TECHNICAL SPECIFICATIONS
Digitization technologies allow offices to control the resolution, size, color, bit-depth and other qualities that affect how the image appears on a computer screen or is output to a printer. Furthermore, once captured, a digital image can be saved in numerous file formats that may or may not include compression technologies that reduce the file size of
the file. Choices offices make in these areas need to be cost-effective while still producing an accessible, accurate, authentic, reliable, legible, and readable record throughout its life cycle.

Convenience copies, those that are not used for preservation but to be used in the office, may be of more diverse formats and resolutions in order to best fit the needs of the office. The office, for example may wish to create JPG or PDFs files from the source files that are of lesser resolution and are compressed for day to day use.

INFORMATION SECURITY AND TRAINING
Departments should appoint a staff member, preferably one with systems administration experience, as the administrator of any digital imaging system. This administrator should be responsible for overall project management, and the development and maintenance of written system documentation which describes the requirements, capabilities, limitations, design, operation, and maintenance of the digital imaging system. All other personnel to be given access to the system should undergo comprehensive training on the system before being granted privileges to add or dispose of records. For security reasons, only personnel who require access to digitized records for their daily job duties should have access to the digital imaging system.

Before creating any digital imaging system, Departments should also consult with UWM Information Security to assess their data classification and determine any additional security needs. See http://infosecurity.uwm.edu for additional information.

DOCUMENT SCANNING PROCESS
Prior to scanning, documents to be imaged should be arranged in such a way that the organization of those documents is clearly discernable. Office personnel in charge of scanning or coordination with scanning vendors should also prepare documents for efficient processing (remove staples, unfold paper, remove extraneous documents, etc.). For the sake of consistency and security, employees responsible for scanning should be specially designated and trained for this purpose.

Once scanning has completed, digital images should be inspected by the system administrator or other responsible party to ensure the accuracy, legibility, and readability of the documents. In cases of scanning projects with very large numbers of documents, a visual quality evaluation of a sample of documents may be appropriate.

LEGAL ISSUES AND RECORDS MANAGEMENT
Records maintained within a digital imaging system are subject to open records requests under Wis. Stat. 19.31-19.39, and must be producible on short notice as required. Wisconsin Administrative Rule 12 outlines six properties that public records in electronic format must maintain:

e) **Accessible:** the record must be able to be located and retrieved in a reasonable amount of time.

f) **Accurate:** the record must correctly reflect the original record when displayed on a retrieval device or reproduced on paper.
g) **Authentic**: the record reflects the creator’s input and can be substantiated.

h) **Reliable**: the record correctly reflects the initial record each time it is produced by the system.

i) **Legible**: The characters within a record can be identified to the exclusion of all other characters.

j) **Readable**: The characters within a record are recognized as words, complete numbers, or symbols.

Records stored within digital imaging systems must be managed according to Wisconsin Stat. 16.61, which requires Records Retention and Disposition Authorities (RRDAs) to be in place for any and all records series created and maintained in the course of University business. RRDAs define a record series, provide a retention period for that series, and give instructions for records disposition (destroy, destroy confidentially, or transfer to Archives). It is recommended that records with temporary disposition be destroyed upon or shortly after expiration, in order to protect records integrity in the event of a security breach.

A partial list of UWM and UW-System RRDAs that apply to campus offices may be found at [http://www4.uwm.edu/libraries/arch/recordsmgmt/common.cfm](http://www4.uwm.edu/libraries/arch/recordsmgmt/common.cfm). If no RRDA exists for a given records series, contact UWM Records Management to have a schedule created. See [http://records.uwm.edu](http://records.uwm.edu) for additional information.

**METADATA INTEGRATION**

Metadata is information associated with digital images that describes the content and structure of the digital image and its context of creation. To increase the accessibility and ease of retrieval of digitized files, metadata should be included within records or linked to them for this purpose.

The creator(s) of the records to be digitized should work with the digitization system administrator and/or vendors to determine what metadata is necessary for appropriate indexing and retrieval of records. A workflow to add this metadata to records at the point of digitization should also be created. Where appropriate, records creators should use controlled vocabularies to increase accessibility and group like documents together.

**STORAGE AND MIGRATION**

It is recommended that source files of digitized records be stored on a network server or as part of an enterprise-wide document management system and NOT on removable media. Appropriate campus IT staff must be notified if the official copy of any public record is to be stored on campus servers. If, for whatever reason, it is not possible to preserve source records on a server, it is recommended that these records be stored on removable WORM (write once, read many: e.g. CD-R, DVD-R) discs only. Rewritable media are generally unacceptable storage media for digitized records because they do not preserve the authenticity (fixity) of records. At least 2 copies of each disk should be made and kept in separate, secure, locations. Be sure to label external storage media with particular care since it is impossible to determine content merely by looking at a disk or tape.
Digital Imaging Systems which contain records with retention periods longer than 5 years should include provision for migrating records, i.e. converting images and indexes to newer file formats or storage media to prevent hardware or software obsolescence. A migration strategy will document how a department will transfer long-term and archival records from one generation of hardware and software to another generation without losing system functionality. The strategy should be written and available with current system documentation.

FOR MORE INFORMATION
Records Management: http://records.uwm.edu
Information Security: http://infosecurity.uwm.edu
Legal Affairs: http://www4.uwm.edu/legal/
Purchasing: http://www4.uwm.edu/bfs/depts/purch/