
interacting with the machine locally. This enables the applications on the shared machine to share data and provides a familiar experience to the users. You can publish a centrally managed, administrative desktop for sensitive workers. This desktop can be prevented from interacting with the remote user's local environment (e.g., so that files on that remote server cannot be downloaded locally).

Desktop Virtualization is in use on Campus in AGREC, CASL, ARHU, FM and Athletics. At scale, the cost for a VDI implementation should run between \$150-\$250/desktop.

In the context of security, this seems most appropriate for use cases where people are spending long periods of time interacting with the sensitive applications.

APPENDIX A

CYBERSECURITY TASKFORCE

Kim L. Colbert	Assistant Director, University Human Resources
Michel Cukier	Associate Professor, Department of Mechanical Engineering; and Director of the Advanced Cybersecurity Experience for Students
Michele Eastman	Assistant President and Chief of Staff
Michael Hicks	Professor, Department of Computer Science
Christian Johnson	Undergraduate Student, Advanced Cybersecurity Experience for Students program
Jonathan Katz	Professor, Department of Computer Science; and Director of Maryland Cybersecurity Center
David Maimon	Assistant Professor, Department of Criminology & Criminal Justice
Dan Navarro	Director of the Office of Academic Computing Services, College of Behavioral and Social Sciences
Porter W. Olsen	Graduate Student, Department of English, Institute for Technology in the Humanities
Terry Roach	Chief Legal Counsel
Apaar Singh	IT Systems Manager, Department of Public Safety
Gerry Sneeringer	IT Security Officer, Division of Information Technology
Michelle L. Straughn	Associate Director, Undergraduate Admissions
Susan Taylor	Professor, Management & Organization Smith School of Business
Amitabh Varshney	Professor, Department of Computer Science; and Director of the Institute for Advanced Computer Studies
Chuck Wilson	Assistant Vice President for Records, Registration and Extended Studies

Ann Wylie	CHAIR TASK FORCE - Professor and Interim Vice President of IT/Chief Information Officer
Jim Zahniser	Executive Director of Information Technology, Clark School of Engineering

SUBGROUP MEMBERS

Robert Maxwell	Security Operations Manager, Division of Information Technology
Kevin Shivers	Senior Security Engineer, Division of Information Technology
Kathy Cavanaugh	Assistant Dean, College of Arts and Humanities
Mike Landavere	IT Director, College of Computer, Mathematical and Natural Sciences
Warren Kelley	Assistant Vice President, Student Affairs
John Zacker	Assistant Vice President, Student Affairs
Jeffrey Hollingsworth	Professor, Department of Computer Science
Erin Howard	Coordinator, Division of Information Technology
Lori Kasamatsu	Coordinator, Division of Information Technology

OTHERS CONSULTED

MITRE	Not-for-profit National Technology Resource
IT Senior Staff	
Michael Brown	Assistant Vice President, Division of Information Technology
Francis LoPresti	Executive Director, Division of Information Technology
Alison Robinson	Assistant Vice President, Division of Information Technology
Tripti Sinha	Assistant Vice President, Division of Information Technology
Phyllis Johnson	Director, Division of Information Technology
Michael Eismeier	Director, Division of Information Technology
IT Council Steering Committee	
Andrew Baden	Professor and Chair, Department of Physics
Paul T. Jaeger	Associate Professor, College of Information Studies
Cynthia Hale	Associate Vice President, Academic Affairs
William Dorland	Professor and Executive Director, Honors College
Jimmy Lin	Associate Professor, College of Information Studies
Jeanne Parker	Assistant Director, Department of Procurement and Supply

APPENDIX B

University

Arizona State University
Arizona State University
Arizona State University
Arizona State University
Arizona State University

Policy

[Access to University Technology Resources & Services Policy](#)
[Information Security Policy](#)
[Border Firewall Policy](#)
[Anti-Virus Standard](#)
[Courtesy Affiliate Standard](#)

Arizona State University	Data Handling Standard
Arizona State University	Data Steward & Trustee Standard
Arizona State University	Incident Response Standard
Arizona State University	Peer-to-Peer (P2P) File Transfer / Copyright Infringement Standard
Arizona State University	Password Standard
Arizona State University	Patch Management Standard
Arizona State University	PeopleSoft Application Data Trustee Standard
Arizona State University	Privileged Accounts Standard
Arizona State University	Risk Assessment and Corrective Action Standard
Arizona State University	Web Development Standard
Arizona State University	Software Development Lifecycle
Arizona State University	Standard Enforcement Exception Request Procedure
Arizona State University	System Audit Requirements
Arizona State University	Web Application Security Standard
Colgate University	Acceptable Use Policy
Colgate University	Stewardship and custodianship of email
Indiana University	Appropriate Use of Information Technology Resources
Indiana University	Misuse and Abuse of Information Technology Resources
Indiana University	Eligibility to Use Information Technology Resources
Indiana University	Privacy of Electronic Information and Information Technology Resources
Indiana University	Excessive Use of Information Technology Resources
Indiana University	Security of Information Technology Resources
Indiana University	Computer and Network Accounts Administration
Indiana University	Extending the University Data Network
Indiana University	Wireless Networking
Indiana University	Use of Electronic Mail
Indiana University	Cyber Risk Mitigation Responsibilities
Indiana University	Web Site Privacy Notices
Indiana University	Information and Information System Incident Reporting, Management, and Breach Notification
Indiana University	Privacy Complaints
Indiana University	Management of Institutional Data
Northeastern	Acceptable Use Policy (AUP) (LINK, 2010-02-25)
Northeastern	Written Information Security Program (PDF, 2013)
Northeastern	InCommon Federation: Participant Operational Practices (PDF, 2012)
Northeastern	Sponsored Account Policy (Link)
Northeastern	myNEU Privacy Policy (Link)
Northeastern	Student Code of Conduct (Link)
Northeastern	SSN and Personal Information Collection, Handling and Use Procedures (PDF, 2010-02)
Northeastern	Retention and Disposition of University Records Policy(PDF, 2012-05-24)

Northeastern	Information Disposal Requirements (PDF, 2009-11)
Northeastern	Identity Theft Prevention Program (PDF, 2009-05)
Northeastern	Management of Copyright Infringement Complaints (PDF, 2009)
Ohio State University	Client Computing Security
Ohio State University	Critical Server Security
Ohio State University	Web Server Security
Ohio State University	Database Server Security
Ohio State University	Local Administrative Privilege
Perdue University	Information Security Policy Document Definitions
Perdue University	Delegation of Administrative Authority and Responsibility
Perdue University	Authentication and Authorization Policy (VII.B.1)
Perdue University	User Credentials Standard
Perdue University	Access Controls Standard
Texas At Austin	Acceptable Use Policy
Texas At Austin	Computer Crimes Law
Texas At Austin	Digital Millennium Copyright Act
Texas At Austin	Enhancing Large Software Purchases (UTS 140)
Texas At Austin	High Value/High Risk Information Technology Purchase Policy (PDF)
Texas At Austin	Information Resources Use and Security Policy
Texas At Austin	Management of UTnet Wireless Access Policy PDF
Texas At Austin	Rate Change Policy PDF
Texas At Austin	Releasing Software as Open Source or Contributing Software to Existing Projects Licensed Under the GNU General Public License PDF
Texas At Austin	University Data Center Security Policy
Texas At Austin	University Electronic Mail Student Notification Policy (Use of E-mail for Official Correspondence to Students) PDF
Texas At Austin	UT System procedure for Enhancing Large Software Purchases (UTS 140)
Texas At Austin	Video and CCTV Security Systems
Texas At Austin	Web Privacy Policy
Texas At Austin	Web Accessibility Policy
Texas At Austin	Data Classification Standard
Texas At Austin	Minimum Classroom Computing Standards (PDF)
Texas At Austin	Minimum Security Standards for Application Development and Administration
Texas At Austin	Minimum Security Standards for Data Stewardship
Texas At Austin	Minimum Security Standards for Merchant Payment Card Processing
Texas At Austin	Minimum Security Standards for Systems
Texas At Austin	UT Domain Name System
Texas At Austin	Data Encryption Guidelines
Texas At Austin	Guidelines for Internal Recruiting of UT Austin IT Employees (PDF)
Texas At Austin	IAM Cloud Integration
Texas At Austin	Network Monitoring Guidelines
Texas At Austin	University Identification Card Guidelines

Texas At Austin	<u>Application for Exception from Use of University of Texas at Austin Central Processing Services</u>	
Texas At Austin	<u>Change Management Process</u>	
Texas At Austin	<u>Secure Web Application Coding Guidelines</u>	W
Texas At Austin	<u>Copyright Violations</u>	
Texas At Austin	<u>Extended List of Category-I Data</u>	
Texas At Austin	<u>ITS Copyright Notice</u>	
Texas At Austin	<u>Network Operations Manual</u>	NE
Texas At Austin	<u>Position of Special Trust</u>	
Texas At Austin	<u>Protecting Data on Vulnerable Devices (Security Practices Bulletin #1)</u>	RI
Texas At Austin	<u>Protecting Sensitive Digital Research Data</u>	
Texas At Austin	<u>Server Security Checklists for System Administrators</u>	
Texas At Austin	<u>Security Exception Reporting</u>	
Texas At Austin	<u>University Login Banner</u>	BA
Texas At Austin	<u>Communications System Design, Construction and Commissioning</u>	
Texas At Austin	<u>Grounding and Bonding for Communications</u>	
Texas At Austin	<u>Hangers and Supports for Communications Systems</u>	
Texas At Austin	<u>Conduits and Backboxes for Communications</u>	
Texas At Austin	<u>Cable Trays for Communications Systems</u>	
Texas At Austin	<u>Firestopping Systems for Communications Cabling</u>	
Texas At Austin	<u>Surface Raceways and Boxes for Communications Systems</u>	
Texas At Austin	<u>Identification for Communications Systems</u>	
Texas At Austin	<u>Optical Fiber Testing and Measurement</u>	
Texas At Austin	<u>Copper Testing</u>	
Texas At Austin	<u>Communications Equipment Room Fittings</u>	
Texas At Austin	<u>Communications Entrance Protection</u>	
Texas At Austin	<u>Communications Termination Blocks and Patch Panels</u>	
Texas At Austin	<u>Communications Optical Fiber Backbone Cabling</u>	
Texas At Austin	<u>Communications Copper Horizontal Cable</u>	
Texas At Austin	<u>Communications Faceplates and Modular Jacks</u>	
Texas At Austin	<u>Communications Patch Cords, Station Cords and Cross Connect Wires</u>	
Texas At Austin	<u>Data Communications Wi-Fi Access Points</u>	
Texas At Austin	<u>Campus Security Systems - Design and Construction Standards</u>	
UMD	<u>Acceptable Use Policy</u>	AU
UMD	<u>University of Maryland Policy on Institutional Data Management</u>	
UMD	<u>University of Maryland Policy on Data Management Structure and Procedures</u>	
UMD	<u>University of Maryland Policy on the Acceptable Use of Information Technology Resources</u>	
UMD	<u>University of Maryland Policy on Gramm-Leach-Bliley Act Information Security Act</u>	
UMD	<u>UMCP Policy on the Collection, Use and Protection of ID Numbers</u>	
UNC - Chapel Hill	<u>E-mail Address Policy</u>	EM
UNC - Chapel Hill	<u>E-mail Domain Policy</u>	DC
UNC - Chapel Hill	<u>Incident Management Policy</u>	

UNC - Chapel Hill	Information Security Policy	
UNC - Chapel Hill	Information Security Liaison Policy	
UNC - Chapel Hill	Institutional Data Governance Policy	
UNC - Chapel Hill	Password Policy for General Users	
UNC - Chapel Hill	Password Policy for System and Application Administrators	
UNC - Chapel Hill	Transmission of Protected Health Information and Personal Identifying Information Policy	
UNC - Chapel Hill	Vulnerability Management Policy	RI
UNC - Chapel Hill	Onyen Policy	
UNC - Chapel Hill	Data Network Acceptable Use Policy	AU
UNC - Chapel Hill	Standards for Electronic Media Disposal	
UNC - Chapel Hill	Data Storage Policy	DA
UNC - Chapel Hill	Wireless Networking Policy	W
UNC - Chapel Hill	Copyright Information and Policies	
UNC - Chapel Hill	Mass E-mail Policy	EM
UNC - Chapel Hill	Special Handling for E-mail Accounts	EM
UNC - Chapel Hill	List Server Policy	
UNC - Chapel Hill	Registering Campus IP Addresses	IP
UNC - Chapel Hill	Registering a Non-UNC Domain Name	DC
UNC - Chapel Hill	Wireless Networking Policy	W
UNC - Chapel Hill	Wireless Spectrum Policy	W
UNC - Chapel Hill	Policy on the Privacy of Electronic Information	
UNC - Chapel Hill	HIPAA Information	
University of Chicago	Acceptable Use Policy for Information Technology	AU
University of Chicago	File Sharing Policy	
University of Chicago	New Information Technologies and Intellectual Property at the University	
University of Chicago	Statement on Commercial and Political Use of IT Resources	
University of Chicago	Use of External Service Providers	
University of Chicago	Policy for the Digital Use of the Social Security Number	
University of Chicago	Policy for Use of the ChicagoID	
University of Chicago	Regulated Computer Policy	
University of Chicago	Policy for Authenticating University of Chicago Users	
University of Chicago	Policy On Computer Account and Email Requirements for University Employees	
University of Chicago	Procedure to Handle Requests for Records or Information	
University of Chicago	Use of Non uchicago.edu Domain Names	
University of Chicago	Redirection of University Domain Names to External Networks	
University of Iowa	Acceptable Use of Information Technology Resources	AU
University of Iowa	Social Security Numbers	
University of Iowa	Video Surveillance Policy	VI
University of Iowa	Network Vulnerability Scanning and Penetration Testing	RI
University of Iowa	Enterprise Active Directory	
University of Iowa	Enterprise Password	PA

University of Iowa	<u>IT Security Incident Escalation</u>
University of Iowa	<u>UI Residence Halls Network (ResNet)</u>
University of Iowa	<u>Network Citizenship</u>
University of Iowa	<u>Mass E-Mail Mailings</u>
University of Iowa	<u>Domain Name Policy</u>
University of Iowa	<u>Email Addresses</u>
University of Iowa	<u>Enterprise Authentication</u>
University of Iowa	<u>Roles and Responsibilities for Information Security</u>
University of Iowa	<u>Backup and Recovery Policy</u>
University of Iowa	<u>Information Security Framework Policy</u>
University of Iowa	<u>Institutional Data Access Policy</u>
University of Iowa	<u>Airspace Policy</u>
University of Iowa	<u>Computer Data and Media Disposal Policy</u>
University of Iowa	<u>Computer Security Breach Notification</u>
University of Iowa	<u>Wireless Networking Policy</u>
University of Iowa	<u>Network Address Allocation Policy for IPv4</u>
University of Iowa	<u>Web Accessibility Policy</u>
University of Iowa	<u>Computer Inventory and Internal Control Policy</u>
University of Iowa	<u>Credit Card Acceptance and Security Policy</u>
University of Iowa	<u>Enterprise Login ID Standard (HawkID)</u>
University of Iowa	<u>Computer Security Standard</u>
University of Iowa	<u>University ID Number Standard</u>
University of Iowa	<u>IT Development Process</u>
Virginia Tech	<u>Acceptable use</u>
Virginia Tech	<u>Security and data protection</u>
Virginia Tech	<u>Identity management</u>
Virginia Tech	<u>Data administration and transparency</u>
Virginia Tech	<u>Infrastructure, architecture, and ongoing operations</u>
Virginia Tech	<u>Project management, acquisition, and deployment</u>
Virginia Tech	<u>Accessibility</u>
Virginia Tech	<u>Acceptable Use and Administration of Computer and Communication Systems</u>
Virginia Tech	<u>Appropriate Use of Electronic Personnel and Payroll Records</u>
Virginia Tech	<u>Alternate Work Site and Telework Policy</u>
Virginia Tech	<u>Sales, Solicitation and Advertising on Campus</u>
Virginia Tech	<u>Use of the Internet and Electronic Communications Systems</u>
Virginia Tech	<u>Acceptable Use of Information Systems at Virginia Tech</u>
Virginia Tech	<u>Policy for Securing Technology Resources and Services</u>
Virginia Tech	<u>Safeguarding Nonpublic Customer Information</u>
Virginia Tech	<u>Policy on Privacy Statements on Virginia Tech Web Sites</u>
Virginia Tech	<u>Privacy Policy for Employees' Electronic Communications</u>
Virginia Tech	<u>Policy for Protecting University Information in Digital Form</u>

Virginia Tech	<u>University Information Technology Security Program</u>
Virginia Tech	<u>University Information Technology Security Program Standard</u>
Virginia Tech	<u>Security Standards for Social Security Numbers</u>
Virginia Tech	<u>Standard for Protecting Sensitive University Information Used in Digital Form</u>
Virginia Tech	<u>Standard for Securing Web Technology Resources</u>
Virginia Tech	<u>Standard for Storing and Transmitting Personally Identifying Information</u>
Virginia Tech	<u>Personal Credentials for Enterprise Electronic Services</u>
Virginia Tech	<u>PID Procedures: Enterprise Electronic Login Credentials</u>
Virginia Tech	<u>Standard for Personal Digital Identity Levels of Assurance</u>
Virginia Tech	<u>Guidelines for Determining the Level of Assurance of Personal Digital Identities</u>
Virginia Tech	<u>Administrative Data Management and Access Policy</u>
Virginia Tech	<u>Standard for administrative data management</u>
Virginia Tech	<u>Interim updates—changes in positions, responsibilities</u>
Virginia Tech	<u>Information Technology Infrastructure, Architecture, and Ongoing Operations</u>
Virginia Tech	<u>Standards for Infrastructure, Architecture, and Ongoing Operations</u>
Virginia Tech	<u>Information Technology Project Management</u>
Virginia Tech	<u>Policy for the Purchase of Department-Based Computer Systems</u>
Virginia Tech	<u>Project Management Standards and Procedures</u>
Virginia Tech	<u>Standard for the Procurement of Information Technology Applications</u>
Virginia Tech	<u>Information Technology Accessibility</u>
Virginia Tech	<u>Accessibility Standards</u>
Virginia Tech	<u>The Virginia Tech Certification Authority (VTCA)</u>
Virginia Tech	<u>The Virginia Tech Certification Authority Certificate Policy</u>
Virginia Tech	<u>Virginia Tech Root Certification Authority Certification Practices Statement</u>
Virginia Tech	<u>Virginia Tech Server Certification Authority Certification Practices Statement</u>
Virginia Tech	<u>Middleware Certification Authority</u>
Virginia Tech	<u>User Certification Authority Certification Practices Statement</u>