

Administrative and Educational Support Report

Information Security

Annual Action Plan Annual Assessment Report

June 2007 – May 2008



Annual Action Plan: June 1, 2007–May 31, 2008

Unit: **IT Division**

UTPA Mission: The University of Texas-Pan American (UTPA) serves the higher education needs of a rapidly growing, international, multicultural population in the South Texas Region. The University preserves, transmits and creates knowledge to serve the cultural, civic, and economic advancement of the region and the state. The University provides students advanced instruction in academic programs offered through innovative delivery systems that lead to professional certification, and baccalaureate, master’s and doctoral degrees. Through teaching, research, creative activity and public service, UTPA prepares students for lifelong learning and leadership roles in the state, nation and world community.

Division: Information Security **Unit Head:** Mauro Scardigno

Unit Mission: The Information Technology Division provides reliable, contemporary, effective, and integrated technology solutions and information services to serve our students and support the mission and goals of the university.

University Goal: Provide students with a quality educational experience that enables them to complete their educational goals in a timely manner.

Division Objective: Enhance, expand and broaden options for students, faculty and staff through excellent and effective information technology solutions.

Unit Objective	Strategy(ies) to Achieve Unit Objective	Measurable Outcome for Unit Objective	Assessment Criteria, Evaluation Methods for Measurable Outcome	New Resources Needed in FY08
Ensure that the current project to maintain and expand centrally managed campus-wide wireless LAN service for all staff, student, faculty, and guest users at UTPA to include outdoor areas and increase density remains secure at all times.	Information Security and Telecommunications will ensure that there is a continued collection and storage of information from the WLAN regarding the location and distribution of wireless users across the campus.	Collected information will allow the Information security staff to quickly identify and resolve issues.	Ensure that the campus-wide WLAN is operating in a secure manner and that the necessary data will continue to be collected from the WLAN system.	No new resources beyond those covered by existing operating funds will be required.

Annual Action Plan June 1, 2007–May 31, 2008

University Goal:

Become an outstanding research institution, emphasizing collaborative partnerships and entrepreneurship.

Division Objective:

Provide infrastructure that will facilitate collaboration and growth among the research community.

Unit Objective	Strategy(ies) to Achieve Unit Objective	Measurable Outcome for Unit Objective	Assessment Criteria, Evaluation Methods for Measurable Outcome	New Resources Needed in FY08
<p>Verify that the design, installation, and utilization of specialized research networks to accommodate grant-funded project requirements in accordance with the terms and conditions set forth by the funding agency such as NASA or the DOD.</p>	<p>Work closely with telecomm support to ensure that telecomm support for research is fully compliant with all of the applicable regulations, UT System rules, State and Federal laws.</p> <p>Work with Telecommunication Services in order to ensure that the network infrastructure is designed to support specialized technological needs and very high levels of security.</p>	<p>Ensure that the network infrastructure is compliant with the technical and security demands of each specific research project and the funding agency that is providing oversight.</p>	<p>Verify that all areas of the network have been properly zoned and firewalled to ensure the most secure virtual environment possible.</p>	<p>No new resources beyond those already designated for this project will be required.</p>
<p>Verify that the expansion of the Internet 2 connection accommodates the needs of research faculty, staff and students.</p>	<p>Work closely with telecomm support during the purchase of additional Internet 2 bandwidth from UT System Office of Telecommunication Services to meet demand</p>	<p>Ensure that the additional Internet 2 bandwidth is compliant with technical and security demands.</p>	<p>Work alongside Telecommunication Services in the process of monitoring bandwidth utilization.</p>	<p>No new resources beyond those already designated for this project will be required.</p>

Annual Action Plan June 1, 2007–May 31, 2008

University Goal:

Optimize institutional effectiveness and efficiency consistent with high quality organizational standards.

Division Objective:

Lead in the delivery of technology solutions resulting in the customer's ability to do things they couldn't do before.

Unit Objective	Strategy(ies) to Achieve Unit Objective	Measurable Outcome for Unit Objective	Assessment Criteria, Evaluation Methods for Measurable Outcome	New Resources Needed in FY08
Maintain and setup high availability edge firewall solution.	Project is currently under way.	Transition rules, modify settings and configuration as required in order to provide efficient network protection.	Ensure that the proper rules continue to be in place and properly backed up.	No new resources beyond those already designated for this project will be required.
Work with Telecommunication Services in the continued effort to secure the network through the ongoing replacement of non-manageable data switches and hubs, as legacy units are discovered, to models supporting port management options.	Continue to assess and examine the campus network to identify and replace non-manageable data switches and hubs.	Working with Telecommunication Services staff, Non-manageable network distribution devices located in the campus network will be replaced with upgraded port manageable versions.	Continue to observe and evaluate the campus network to identify non-manageable network devices.	No new resources beyond those covered by existing operating funds will be required.
Ensure that all of the communications closets and switch rooms have standardized locksets with only designated Video Resources, Telephone Services, and	Project is currently under way.	All communication closets and switch rooms will have standardized locksets that will limit entry to certain designated Video Resources, Telephone	Ensure and work alongside Telecommunication Services to verify that all comm closet and switch room locksets function with a single keyset or fob (electronic key). Provide the means to produce an audit trail for all	No new resources beyond those already designated for this project will be required.

Annual Action Plan June 1, 2007–May 31, 2008

Unit Objective	Strategy(ies) to Achieve Unit Objective	Measurable Outcome for Unit Objective	Assessment Criteria, Evaluation Methods for Measurable Outcome	New Resources Needed in FY08
Network Services technicians plus UTPA Police and Physical Plant staff having access.		Services, and Network Services technicians plus UTPA Police and Physical Plant staff.	entries.	
Maintain the current spam filtering solution.	Ensure that the commercially available solution will continue to provide satisfactory filtering services.	Implement new rules, modify settings and configuration as required in order to provide efficient spam filtering.	Ensure that the proper rules continue to be in place and properly backed up.	No new resources beyond those already designated for this project will be required.
Ensure and verify the continued effort to map all switched ports on campus to a physical location.	Network staff will trace all unmarked data cables attached to switched ports to their physical end-points and label them appropriately and enter the information in a database.	All switched ports will be mapped to physical locations allowing network and security technicians to quickly identify, locate and resolve issues.	Work along side Telecommunication Services to ensure that all wired connections to the UTPA network have been mapped and appropriately stored in a searchable database.	No new resources beyond those covered by existing operating funds will be required.
Provide continuing additional direct support to Support Services and Systems team.	Information Security staff will continue to collaborate with Support Services and Systems Team in the deployment of additional security measures and across the campus including: <ol style="list-style-type: none"> 1. Strong passwords 2. Additional encryption solutions for portable devices. 3. Encrypted server data storage 	<ol style="list-style-type: none"> 1. Strong passwords. 2. Additional encryption solutions for portable devices. 3. Encrypted server data storage. 	Evaluate, recommend and possibly obtain encryption solutions and further define and enforce strong password implementation policies In conjunction with Support Services and System teams.	<p>Approximately \$20,000 will be needed to manage password policies across systems.</p> <p>Information security will approximately need \$15,000 to deploy additional portable encryption solutions.</p> <p>Information security will approximately need \$100,000 for a partial deployment of encrypted server data storage.</p>
Provide continuing	Information Security staff	4. PIX firewall	Continue to monitor the operation	No new resources

Annual Action Plan June 1, 2007–May 31, 2008

Unit Objective	Strategy(ies) to Achieve Unit Objective	Measurable Outcome for Unit Objective	Assessment Criteria, Evaluation Methods for Measurable Outcome	New Resources Needed in FY08
<p>additional direct support to the Telecommunication Services Staff.</p>	<p>will continue to collaborate with the Telecommunication Services for the deployment of additional security measures and equipment across the campus network including:</p> <ul style="list-style-type: none"> 4. edge firewall installation 5. enhanced VPN solution 6. NAC implementation 7. additional PIX firewall deployments 	<p>deployments</p> <ul style="list-style-type: none"> 5. Edge Firewall installation 6. Enhanced VPN solution implementation 7. NAC deployment 	<p>of the Cisco PIX firewalls and their performance.</p> <p>Properly functioning campus firewall.</p> <p>Complete VPN/NAC evaluation and make recommendation for purchase.</p>	<p>beyond those already provided are needed for the campus edge firewall project.</p> <p>Approximately \$50,000.00 (rough estimate) will be needed to purchase a VPN/NAC solution.</p> <p>No new resources are required for PIX firewall deployments.</p>

FY08 AES Assessment Results Report

UTPA

Admin - Information Security

Unit Mission: The Information Technology Division provides reliable, contemporary, effective, and integrated technology solutions and information services to serve our students and support the mission and goals of the university.

Unit Head: Mauro Scardigno

Division: Division of Information Technology

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
<p>Admin - Information Security - Managed Campus-wide Wireless LAN - We will ensure that the current project to maintain and expand centrally managed campus-wide wireless LAN service for all staff, student, faculty, and guest users at UTPA to include outdoor areas and increase density remains secure at all times.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Information Security and Telecommunications will ensure that there is a continued collection and storage of information from the WLAN regarding the location and distribution of wireless users across the campus. 2. Assist Telecommunication Services with the creation of any necessary policies applicable to the use of wireless equipment.</p>	<p>Assessment Method: Ensure that the campus-wide WLAN is operating in a secure manner and that the necessary data will continue to be collected from the WLAN system.</p> <p>Criterion for Success: Collected information will allow the Information security staff to quickly identify and resolve issues.</p>	<p>09/12/2008 - 100% complete. This is an ongoing process.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This is an ongoing process</p>
<p>Admin - Information Security - Verify the design, installation, and utilization of specialized research networks - We will verify that the design, installation, and utilization of specialized research networks to accommodate grant-funded project</p>	<p>Assessment Method: Ensure that the network infrastructure is compliant with the technical and security demands of each specific research project and the funding agency that is providing oversight.</p>	<p>09/12/2008 - 100% complete. This is an ongoing process.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This is an ongoing process</p>

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
<p>requirements in accordance with the terms and conditions set forth by the funding agency such as NASA or the DOD.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Work closely with telecomm support to ensure that telecomm support for research is fully compliant with all of the applicable regulations, UT System rules, State and Federal laws. 2. Work with Telecommunication Services in order to ensure that the network infrastructure is designed to support specialized technological needs and very high levels of security.</p>	<p>Criterion for Success: Ensure that the network infrastructure is compliant with the technical and security demands of each specific research project and the funding agency that is providing oversight.</p>		
<p>Admin - Information Security - Verify Network Expansion - We will verify that the expansion of the Internet 2 connection accommodates the needs of research faculty, staff and students.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Work closely with telecomm support during the purchase of additional Internet 2 bandwidth from UT System Office of Telecommunication Services to meet demand. 2. Assure that security equipment is</p>	<p>Assessment Method: Work alongside Telecommunication Services in the process of monitoring bandwidth utilization.</p> <p>Criterion for Success: Ensure that the additional Internet 2 bandwidth is compliant with technical and security demands.</p>	<p>09/12/2008 - 100% complete. This is an ongoing process.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - Part of the ongoing process</p>

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
properly updated and funded to support any proposed bandwidth increase.			
<p>Admin - Information Security - Maintain Edge Firewall Solution - We will maintain and setup high availability edge firewall solution.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Continue to improve on setup of the high availability firewall solution as new features become available. 2. Utilize the high availability firewall to segregate networks as need or required by policy. 3. Continue to tune intrusion prevention features and rules to minimize security risks. 4. Establish and communicate standard operating procedures for firewall rule exceptions.</p>	<p>Assessment Method: Ensure that the proper rules continue to be in place and properly backed up.</p> <p>Criterion for Success: 1. Modify settings and configuration as required in order to provide efficient network protection. 2. Successfully tune firewall settings. 3. Successfully deploy PIX firewalls as needed 4. Successfully implement monitoring & store PIX firewall events</p>	<p>09/12/2008 - 100% completion. Rules and configuration settings have been modified as needed. This is an ongoing process.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This is an ongoing process</p>
<p>Admin - Information Security - Work with Telecommunication Services to Secure Networks - We will work with Telecommunication Services in the continued effort to secure the network through the ongoing replacement of non-manageable data switches and hubs, as legacy units are discovered, to models supporting port management options.</p> <p>Outcome Types: Administrative - Fiscal Year 2008</p>	<p>Assessment Method: Continue to observe and evaluate the campus network to identify non-manageable network devices.</p> <p>Criterion for Success: Working with Telecommunication Services staff, Non-manageable network distribution devices located in the campus network will be replaced with upgraded port manageable versions.</p>	<p>09/12/2008 - 100% complete. Discovered devices have been replaced. This is an ongoing process.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This is an ongoing process</p>

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
<p>Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Continue to assess and examine the campus network to identify and replace non-manageable data switches and hubs. 2. Create and maintain a database of open port activity on campus wide machines.</p>			
<p>Admin - Information Security - Ensure that Communication Closets are Secure - We will ensure that all of the communications closets and switch rooms have standardized locksets with only designated Video Resources, Telephone Services, and Network Services technicians plus UTPA Police and Physical Plant staff having access.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p>	<p>Assessment Method: Ensure and work alongside Telecommunication Services to verify that all comm closet and switch room locksets function with a single keyset or fob (electronic key). Provide the means to produce an audit trail for all entries.</p> <p>Criterion for Success: All communication closets and switch rooms will have standardized locksets that will limit entry to certain designated Video Resources, Telephone Services, and Network Services technicians plus UTPA Police and Physical Plant staff.</p>	<p>09/12/2008 - 50% completion. Mechanical rooms need to be completed.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This project will continue during the next fiscal year.</p> <hr/>
<p>Admin - Information Security - Maintain the Spam Filtering Solution. - We will maintain the current spam filtering solution</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Ensure that the commercially available</p>	<p>Assessment Method: Ensure that the proper rules continue to be in place and properly backed up.</p> <p>Criterion for Success: Implement new rules, modify settings and configuration as required in order to provide efficient spam filtering.</p>	<p>09/12/2008 - 100% completion. Rules and configuration changes have been added and modified accordingly. This is an ongoing process.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This is an ongoing process.</p> <hr/>

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
<p>solution will continue to provide satisfactory filtering services.</p>			
<p>Admin - Information Security - Ensure and Verify the Efforts to Map Switched Ports - We will ensure and verify the continued effort to map all switched ports on campus to a physical location.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Network staff will trace all unmarked data cables attached to switched ports to their physical end-points and label them appropriately and enter the information in a database.</p>	<p>Assessment Method: Work along side Telecommunication Services to ensure that all wired connections to the UTPA network have been mapped and appropriately stored in a searchable database.</p> <p>Criterion for Success: All switched ports will be mapped to physical locations allowing network and security technicians to quickly identify, locate and resolve issues.</p>	<p>09/12/2008 - 43% of all buildings have been mapped. This is process will continue during the next fiscal year.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This is an ongoing process</p>
<p>Admin - Information Security - Provide Continuing Support to Support Services and Systems Team - We will provide continuing additional direct support to Support Services and Systems team.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Information Security staff will continue to collaborate with Support Services and Systems Team in the deployment of additional security measures and across the campus including:</p>	<p>Assessment Method: Evaluate, recommend and possibly obtain encryption solutions and further define and enforce strong password implementation policies In conjunction with Support Services and System teams.</p> <p>Criterion for Success: 1. Strong passwords. 2. Additional encryption solutions for portable devices. 3. Encrypted server data storage.</p>	<p>09/12/2008 - Strong passwords have been implemented. Encryption recommendation for portable devices has been provided. Additional encryption solutions will continue to be evaluated during the next fiscal year. Data storage solutions continue to be evaluated.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - Projects will continue to be worked on during next fiscal year.</p>

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
<ul style="list-style-type: none"> - Strong passwords - Additional encryption solutions for portable devices. - Encrypted server data storage - Campus wide on-line security training - Provide professional training to support and systems staff when economically feasible 			
<p>Admin - Information Security - Provide Continuing Support to the Telecommunication Services Staff. - We will provide continuing additional direct support to the Telecommunication Services Staff.</p> <p>Outcome Types: Administrative - Fiscal Year 2008 Administrative - Fiscal Years 2009 - 2011</p> <p>Start Date: 06/01/2007</p> <p>Outcome Status: Active/Ongoing</p> <p>Strategies: 1. Information Security staff will continue to collaborate with the Telecommunication Services for the deployment of additional security measures and equipment across the campus network including: <ul style="list-style-type: none"> - edge firewall tuning - enhanced VPN solution with the use of two factor authentication - NAC implementation - additional PIX firewall deployments - monitor internal activity between core routing equipment - setup a research environment for testing and forensic analysis - implementation of a solution to monitor & store PIX firewall events - obtain a replacement for dynamic host </p>	<p>Assessment Method: Continue to monitor the operation of all firewalls and their performance Complete VPN/NAC evaluation and make recommendations. Complete the evaluation of log analysis solutions Research methods for monitoring internal activity between core routing equipment Setup a research environment for testing and forensic analysis Obtain a replacement for dynamic host blocking in the student networks Continue to seek alternatives for outsourcing student networks</p> <p>Criterion for Success: 1. Successfully tune firewall settings. 2. Successfully implement a VPN solution with the use of two factor authentication 3. Successful NAC implementation 4. Successfully deploy PIX firewall as needed 5. Successfully implement monitoring of internal activity between core routing equipment 6. Successfully setup a research environment for testing and forensic analysis 7. Successfully implement monitoring & store PIX firewall events 8. Replace the current dynamic host</p>	<p>09/12/2008 - Edge firewal deployment was completed. Pix firewall setups have been deployed as needed. VPN solution has been evaluated. NAC evaluation and deployment will continue during next fiscal year.</p> <p>Result Type: Criterion Met</p> <p>Next Step: Continue Current Strategy(s)</p>	<p>09/12/2008 - This will continue during the next fiscal year.</p>

Intended Outcomes	Means of Assessment & Criteria for Success / Tasks	AES Assessment Results	Use of Result & Follow-Up
blocking in the student networks - continue to seek alternatives for outsourcing student networks	blocking in the student networks 9. Outsoure student networks	09/12/2008 - Edge firewal deployment was completed. Pix firewall setups have been deployed as needed. VPN solution has been evaluated. NAC evaluation and deployment will continue during next fiscal year. Result Type: Criterion Met Next Step: Continue Current Strategy(s)	09/12/2008 - This will continue during the next fiscal year.