IT Policies

* E-discovery

Scope

University of Arkansas at Little Rock shall be responsive to all legal requests for electronically stored information (ESI) from any recognized legal authority. The University maintains numerous logs, records, backups and other forms of data that may be requested in a litigation process. The University will not voluntarily provide any such information; data will only be released under the terms of a court ordered disclosure, subpoena or other appropriate request. Unless compelled to silence by the request, University of Arkansas at Little Rock shall advise the subject of an ESI order of the existence of the request. Data collection, preservation and production shall proceed as requested and will be provided unless the subject seeks and obtains injunctive relief from the request.

Policy Statement

All legal orders involving electronic data shall be expeditiously sent to the Chief of Information Technology Officer. If the request has not been reviewed by the university legal counsel, the Information Security Officer may request a review or clarification of the order. Legal counsel may determine if there is a need for a Litigation Hold Notice, the scope of the Hold to be issued, and formally issue a Litigation Hold Notice.

In conjunction with the legal counsel, the Chief of Information Technology Officer shall (1) identify the ITS and records management personnel who can assist in protecting and preserving ESI and other relevant information; (2) identify the specific individuals (end users) who may have responsive ESI; (3) identify the categories of information that are to be preserved or; (4) utilize an ESI questionnaire or discovery survey to facilitate the location of ESI. Additionally, the legal counsel and the Chief of Information Technology Officer shall review collected ESI to determine if it is responsive and/or subject to evidentiary privileges; identify and segregate confidential information and release the data as appropriate.

Reason for Policy

It is very important that ESI is preserved in its original electronic form so that all information contained within it, whether visible or not, is also available for inspection. This means that requested data on a local or external disk drive may require that the entire disk drive be preserved intact to comply with the request. Costs to recover, process and protect ESI are typically borne by the party that holds the data. Preservation costs can also be impacted by the form in which it must be maintained. ESI that imposes an undue burden or cost to make it accessible need not be provided initially, but may later need to be produced, as determined on a case-by-case basis. Examples of ESI data that might not be reasonably accessible include: information backups created for disaster recovery, legacy information from technically obsolete systems, remnants of deleted information that would require the aid of forensic specialists to recover, and databases designed to produce information only in ways not useful to the case. If costs to produce ESI are excessive, the university reserves the right to request relief from the court of jurisdiction.

Procedures

If you receive any legal request from an outside agency for ESI, you should make a copy of the request for your records and forward the original request to the Information Security Officer. If you receive a request from the Chief of Information Technology Officer or the university legal counsel, you must acknowledge receipt of the request, comply with all instructions and preserve all requested information. In general, the end user should:

Suspend all personal practices regarding the destruction of ESI related to the Hold (e.g., deletion of emails, voice mail, drafts of documents, accessing a document that may be altered by opening it, etc.)

If possible, disable all known automated functions that affect the preservation of the requested ESI (e.g., automatic deletion of emails, folder creation, etc.). If this is not possible, contact ITS to disable these functions

Contact the Chief of Information Technology Officer or university legal counsel when needing access to a document or file containing ESI that may be relevant to the Hold

Identify location of all potentially responsive information; provide relevant computers/devices

Definitions

Electronically Stored Information (ESI)—All electronically stored information and data subject to possession, control, or custody of an institution regardless of its format and the media on which it is stored. ESI includes, but is not limited to: electronic files; communications, including email and instant messages sent or received, and voicemail; data produced by calendaring software; and information management software. In addition to specific data that are electronically stored and readily retrievable, ESI includes data that may not be visible that is generated by computer hard-drive, email and instant messaging, information management software, handheld computer devices (ex: Blackberry), telecommunications devices, and back-up storage devices. ESI may be stored on different electronic devices and removable devices (ex: internal and external drives, PDAs, smart phones, servers, laptops, backup tapes, thumb drives, CDs, DVDs) and may also reside at different locations (e.g., on the home or work systems, institutionally-owned or personal systems, in departmental files, etc.).

1. Data Files:
   - Active
   - Archived
   - Backups
   - Legacy
   - Internet (Web)
2. System Files:
   - Audit trails
   - Access control lists
   - Metadata
   - Logs
   - Internet "Footprints"
     - Cookies
     - Internet History
     - Browser Activity
3. Electronic Communications
   - Email
   - Instant messages

Sources may include:

1. Hardware Devices (Samples)
   - Servers
   - Desktops
   - Laptops
   - Personal Digital Assistants (PDA)
   - Mobile Phone
   - USB Drives
   - Network appliances
   - Storage area Networks (SANS)
   - Backup Media (e.g., CD, tape)
   - Internal and external disk drives
   - MP3 / IPOD players
2. Software Applications (Samples)
   - ERP systems
   - CRM Systems
   - Financial / Accounting Systems
   - Student Information Systems
   - e-Learning Management Systems
   - Software application code
   - Email systems / service
   - Voicemail systems
   - Instant messaging system / service
   - Calendaring systems
   - Network activity monitoring systems
   - Third-party systems? (e.g., ISP, outsourcer, etc)
   - Archiving / Records Management systems (e.g., Filenet)
   - Collaboration systems
   - Database various
   - Spreadsheets

Locations may include:

- Work devices, applications and departments
- Home devices and applications
- Third-party devices and applications – It is critical to understand what institutional data is held by third-parties and the terms of the contracts and other arrangements that govern access to such data should it ever be required as part of a Litigation Hold Notice.

Sanctions

Procedures has to be followed according to this policy.

Additional Contacts

Legal Department.

Chief of Information Technology Officer

* Information security policy for research

Scope

Research data include information that is collected or generated by researchers, information that is obtained from third parties pursuant to Data Use Agreements (DUAs) and third party information that is not subject to DUAs. This Policy covers research data that are confidential, by reason of regulation, policy, law, or contractual obligation.

Policy Statement

Confidential research data must be protected in a manner that complies with applicable law and regulation, agreements covering the acquisition and use of the data, and, as applicable, University policies, such as those pertaining to human subject's research. To protect research data appropriately and efficiently, the University's researchers, Institutional Review Boards, and Information Security Officers must understand and carry out their responsibilities related to data security. The basic principle of this Policy is that more exacting security measures must be followed as the information risk posed by a research project increases. The principle is embodied in a set of security levels and accompanying sets of protective measures. While the measures pertain to computer and network security for digital data, this basic approach, in which security measures are calibrated to risk, should guide researchers' plans for handling and storage of paper records, and IRBs' review and approval of those plans.

This policy applies to all research data physically housed at the University of Arkansas at Little Rock, regardless of ownership. When UALR researchers collect or store research data at other facilities at the request of the researcher, consult with the outside facility IT staff and, as appropriate, inspect the outside facility to assess whether security measures are concordant with this policy.

Reason for Policy

UALR's Information Security Policy effectively addresses the need to protect confidential and sensitive information that is maintained in the various spheres of University administration. Nevertheless, the research setting poses particular information security risks and has regulatory and contractual constraints that require additional policy provisions and protective measures.

Procedures

This policy covers data security requirements for human subjects' research and when DUAs contain confidentiality or data protection provisions.

Human Subjects' Research

1. When applying for the Graduate School approval, the researcher will describe any personally identifiable information that will be collected from subjects, how the information will be collected, the number of subjects, promises or representations regarding confidentiality made to subjects in recruitment materials and consent forms, and measures to protect the confidentiality of information, such as maintaining a key code or physical security provisions for paper records.
2. The Graduate School will consult with the researcher, obtain additional information as needed, assign a security level to the project, and provide the researcher with the Requirements document for the level (see Related Documents).
3. After reviewing the Requirements document, the researcher will, if necessary, consult with ITS in order to implement the security level requirements.
4. When the researcher has met physical, network, and system security requirements and put in place required operational procedures, the researcher shall so attest to the Graduate School, by submitting the Researcher Attestation Form or in another manner satisfactory to the Graduate School.
5. Upon receipt of the attestation of the researcher, the Graduate School may complete its approval process. When a researcher requires proof of the Graduate School approval before security requirements are satisfied, the Graduate School can approve subject to the condition that no human subjects' data will be acquired until the researcher has met the security requirements and so attested to the Graduate School.
6. In addition to the researcher's attestation, the Graduate School may also request confirmation from ITS Information Security that security requirements have been satisfied, in order to complete its approval process.

Definitions

Data Use Agreement: Any agreement between a data provider and a researcher who requests the data concerning the transfer, use, security, or disposal of the data, regardless of the title or form of the agreement.

Facility: Any computer or computer network and the office or laboratory in which it is situated, used for the processing and storage of research data.

Human Subjects' Research: research that involves obtaining data about a living individual through intervention or interaction with the individual, or obtaining identifiable private information about the individual.

Sanctions

This Policy applies to researchers and research team members who obtain or generate information that is confidential, in particular personally identifiable human subject information and information that is subject to Data Use Agreements (DUAs) containing confidentiality and information security provisions. The Policy also applies to the Institutional Review Boards and Chief of Information Technology Officers who are responsible for working with researchers and research team members to ensure that risks associated with human subjects research information within the scope of the Policy have been identified, assessed, and addressed.

Additional Contacts

* Payment card processing

Scope

The purpose of this policy is to establish guidelines for processing charges/credits on Credit Cards to protect against exposure and possible theft of account and personal cardholder information that has been provided to the University of Arkansas at Little Rock; and to comply with the Payment Card Industry's Data Security Standards (PCI) requirements for transferring, handling and storage of credit card information. This policy applies to all University of Arkansas at Little Rock employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format. Affiliated corporations are encouraged to comply.

Policy Statement

All transactions (including electronic based) that involve the transfer of credit card information must be performed on systems approved by the University's Office of the Treasurer, after a prior compliance and security review from Information Technology Services. All specialized servers approved for this activity must be housed within the Department of Information Technology and administered in accordance with the requirements of all University of Arkansas at Little Rock policies and the Cardholder Information Security Program (CISP). University of Arkansas at Little Rock is involved in PCI DSS compliance and is subject to examination of system security and configuration to ensure cardholder information is securely maintained. The Treasury Operations Office will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through Data Capture / Point of Sale machines (Credit Card Terminals), while Web Based procurement of credit cards will be monitored by the Business analyst of Information Technology. In addition:

A. No electronic credit card numbers should be transmitted or stored in any other system, personal computer, or e-mail account.

B. Physical cardholder data must be locked in a secure area, and limited to only those individuals that require access to that data. In addition, restrict access to data on a "need to know" basis.

C. Store only essential information. Do not store the Card Validation Code, or the PIN Number. Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.)

D. Stored credit card information will be retained for a maximum of 60 days. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.

E. Departments must comply with the PCI Data Security Standard Payment Card Industry Data Security Standard

F. Exceptions to this policy may be granted only after a written request from the unit has been reviewed and approved by the University Office of the Treasurer.

Reason for Policy

Procedures

Confidentiality and Security of Account Information

University of Arkansas at Little Rock employees are governed by various policies that include the Code of Conduct, Acceptable Use, Information Security policies, the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach Bliley Act (GLBA), and the Red Flag Policy. These policies include the responsibility to protect the confidentiality of individual's personal information. All credit card & debit card transactions, including web based procurement of the same, must be initiated and controlled through the Office of the Treasurer.

Departments, who need to accept credit/debit cards and obtain a physical terminal to either swipe or key transactions through that Data Capture machine, need to contact the Executive Director of Treasury Operations to execute the required paper work, obtain a Merchant Number, receive training, and be given direction as how to journalize those transactions on the books of the University. Departments wishing to engage in electronic commerce are required to use UALR's E-Pay. After contacting the Executive Director of Treasury Operations, a specialized Merchant Number will be established, and the department will be directed to the Business Analyst of Information Technology who will provide technical instructions and documentation. Requesting departments must also inform Financial Reporting's Senior Bookkeeper in the Controllers Department of newly requested and processed accounts for credit card devices. Departments will be responsible for creating their own web site "storefront" with assistance from Information Technology's Business Analyst for integration with E-Pay. Once the storefront program passes required payment parameters to UALR, secure payment, E-Pay, will be executed. Approval codes and other related elements will be returned to the originating web site. In addition, the accounting of journal entries will be automatically processed.

The practice of least privilege will be utilized to restrict access to sensitive data. This practice involves assigning individual access on a "need-to-know" basis. Positions requiring specific levels of data access will be provided with approval by the department head and IT. For employees without a "need to know", credit card account numbers will be masked to protect account information. The first six and last four digits are the maximum number of digits to be displayed. Under no circumstances will it be permissible to obtain credit card information or transmit credit card information by e-mail. Under no circumstances will any other payment mechanism other than E-Pay be Permissible for electronic commerce on the web. Exceptions to this procedure must be submitted in writing to the University's Office of the Treasurer. Any changes to systems housing account information must only be performed When: Thorough testing has taken place to ensure adequacies of controls; Functionality testing with clients has taken place; required client training is completed; Change control processes have been followed.

Enforcement by Information Technology Services Chief of Information Technology Office: Responsible for approving installation, modifications, and removal of all network hardware devises throughout UALR Campus; Responsible for monitoring the enforcement of this policy.

System Administrators: Responsible for granting permission to sensitive areas based on the principle of least privilege; Responsible for configuring the masking of account numbers based on a user's access.

Data Storage and Destruction

The following processes must be followed for all data storage and destruction:

Hardcopy containing cardholder data will be destroyed immediately after processing.

All electronic media containing cardholder information should be labeled and identified as confidential.

An inventory of media containing cardholder information should be performed monthly.

Audit logs for system housing cardholder data will be available for a period of four (4) years.

Electronic backup media containing cardholder data will be available for a period of four (4) years and then properly erased or decommissioned and destroyed on a monthly basis.

Definitions

Cardholder Information Security Program (CISP): Visa's Cardholder Information Security Program (CISP) is designed to ensure that all merchants that store, process, or transmit Visa cardholder data, protect it properly. To achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.

PCI: The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

Cardholder Data: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, and address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Card member ID (Discover) or CID - Card Identification Number (American Express) (e.g., three- or four-digit value printed on the front or back of a payment card.

System Administrator / Data Custodian: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and Permanent part-time employees of the University and/or third party vendors approved by IT and/or Treasury Operations may function as system/network administrators and/or data custodians.

Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of physical and or electronic payment capability for affected units. Additionally, fines may be imposed by the affected credit card company, beginning at $50,000 for the first violation. Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities. Violations of the policy will be addressed by the individual's respective disciplinary policies and procedures. All known and/or suspected violations must be reported to the applicable Network/System Administrator who will report, as appropriate, to the Information Technology Services Department. The appropriate University administrative office will investigate all such allegations of misuse with the assistance of the Department of Information Technology Services, Treasury Operations, General Counsel, and the Department of Human Resources.

Additional Contacts

* Student computer ownership

Scope

All new students who attend Illinois State University after the fall semester of 2005 must bring with them a personal Computer that meets the University's published minimum hardware and software standards.

Policy Statement

University of Arkansas at Little Rock has approved a requirement each student new to the university is expected to own a computer that meets the University's published minimum hardware and software standards. For mobility and flexibility reasons, laptops are strongly recommended. No student will be prevented from attending classes based on an inability to purchase a computer; the cost of a computer can be added to the student's total cost of attendance. The cost of attendance is one of the factors that determine the amount of financial aid offered. Campus-wide minimum standards for a computer workstation are updated each year. Additional requirements may be differentiated by major or academic program. This information may be found on the web site. The University provides a comprehensive support infrastructure to help students with purchasing computers, installation, trouble-shooting, and training. These services include Residential Computer Consultants (RCCs), Help Desk support, high-speed Internet ports in residence hall rooms, and wired and wireless data ports in social and library study areas around campus to support mobile computing.

Financial Aid Summary

While the computer requirement imposes an additional financial obligation on students, there are several solutions and means to make it affordable and practical for students, especially low-income students. Computer ownership costs and expenses can be added as a component in the University's Cost of Attendance for entering freshman and undergraduate transfer students.

Students may apply for financial aid to help cover the cost of a computer by completing and submitting the Free Application for Financial Aid (FAFSA) for the appropriate academic year. Students and parents should check with IT Services to obtain a price quote for an appropriate computer. If financial assistance is needed in addition to the initial amount of aid offered, IT Services will refer students to the Financial Aid Office to request a budget adjustment. Information is also available at IT Services for private financing options.

Computer Acquisition Options

IT Services, a department of the University, provides information and access to special pricing for the acquisition of computers. Special software licensing programs are also available. After consulting with IT Services, the following options for acquiring a computer may be considered:

1. Purchase a new computer. The University continuously works with selected vendors to help provide students with aggressively priced hardware and software. Special bundles with University configurations usually offer the best pricing.
2. Purchase a used computer. The University partners with one or more vendors that make available used equipment.
3. Bring an existing computer. The specifications should be matched against the University's current requirements.
4. Apply for use of a personal computer through the granting program for those students in need. The University seeks corporate and individual donors who contribute towards a limited pool of computers which are loaned and then granted to students on a semester basis.

Reason for Policy

Procedures

This policy will be periodically reviewed by the Information Technology Services and changes or additions to this policy will be recommended by this Council to the President of the University. Information technology resources and systems are changing rapidly both in terms of technology and application, and the University reserves the right to amend this policy at any time. The version posted on the web at www.policy.ilstu.edu/ is the governing policy.

Definitions

Sanctions

Additional Contacts

* Web accessibility

Scope

Policy Statement

All new and Redesigned Web Pages published by any UALR college, school, department, program, or unit on or after the effective date of this policy must conform to the United States Access Board's Electronic and Information Technologies Accessibility Standards and this policy. All Legacy Web Pages published prior to the effective date of this policy must conform to these accessibility standards. The time frames for achieving compliance are included in the Procedures section of this policy. Progress toward achieving and maintaining fully accessible Web pages must be documented on annual status reports.

This policy applies to all official Web pages and associated Web-based services developed by or for a college, school, department, program, or unit of Purdue University. Nothing in this policy is intended to prevent the use of designs or technologies as alternatives to those prescribed in the standards, provided they result in substantially equivalent or greater access to and use of a Web site by people with disabilities.

Reason for Policy

The creation and dissemination of knowledge is a defining characteristic of universities and is fundamental to UALR's mission to promote learning, discovery, and engagement. The use of digital and Web-based delivery of information is increasingly central to carrying out the University's mission. Acknowledging this fact, UALR is committed to ensuring equal access to information for all its constituencies.

This policy establishes minimum standards for the accessibility of Web-based information and services considered necessary to meet the University's goal and ensure compliance with applicable law.

Procedures

Compliance Requirements and Time Frames

1. All new and Redesigned Web Pages published on or after the effective date of this policy must be in compliance with the U.S. Access Board's Electronic and Information Technologies Accessibility Standards and must indicate in plain text a method of contact for users with disabilities having trouble accessing content within the site. The contact information is typically a phone number and/or e-mail address that

puts the user in touch with the person(s) responsible for the content and function of the page who can usually reply within one business day

2. By July 1, 2010, all Legacy Web Pages must indicate in plain text a method of contact for users with disabilities having trouble accessing content within the site as outlined in Section A above.

3. In addition to Section B above, all Legacy Web Pages must be revised to be in compliance with the U.S. Access Board's Electronic and Information Technologies Accessibility Standards. Priority must be given to creating accessible Web pages for core institutional information pertaining to students, faculty, staff, alumni, retirees, and visitors. Units with large Web sites containing core institutional information must establish priorities for ensuring access to these pages based on time, sensitivity of function, and frequency of use. Decisions regarding the order in which Legacy Web Pages are revised are made by following the implementation priorities below. Each college, school, department, program, or unit of the University is responsible for determining which of their Legacy Web Pages fall into the percentages listed.

    1. The top 25% of Legacy Web Pages that are used most frequently (i.e., that get the largest number of hits) must be in compliance within one year of the effective date of this policy.

    2. Pages required for participation, funding, disability-related services, and other key pages needed by individuals with disabilities not already in the top 25% must also be in compliance within one year of the effective date of this policy.

Specific Requests for Access

Upon specific request for access by an individual with a disability, Legacy Web pages must be made accessible, or an equally effective alternative provided, within 10 business days of receiving the request. The unit responsible for the creation and maintenance of the information on the Web page is responsible for making it accessible. Equally effective means that the alternative communicates the same information in as timely a fashion as does the original Web page. For interactive or service pages, equally effective means that the end result (e.g., registration) is accomplished in a comparable time and with comparable effort on the part of the requestor. If the context of the information or service the page provides cannot be made accessible within 10 business days, this timeframe may be extended.

Upon specific request for access by an individual with a disability, Archive Web Sites and Pages containing core administrative or academic information, official records, or similar information must be updated to be in compliance or the content of the Web page(s) must be made available by another means that is accessible to the individual. The unit responsible for the creation of the information on the page(s) is responsible for providing that access within 10

business days of receiving the request. If the context of the information or service the page provides cannot be made accessible within 10 business days, this timeframe may be extended.

Reporting

Status reports must be submitted annually no later than April 1 by each college, school, department, program, or unit of UALR to their campus Equal Opportunity Officer. The report must summarize the efforts toward achieving and maintaining fully accessible Web pages, as defined by this policy. Efforts and accomplishments over the previous year, as well as targets for the upcoming year, must be included in each report.

Policy Review

The Office of the Vice President for Ethics and Compliance will initiate a review of and make necessary revisions to this policy at least once every two years with the input of a review group. The review group will include, but not be limited to, designees from the Office of Institutional Equity, Office of the Vice President for Information Technology Services, Disability Resource Center.

Definitions

Archive Web Site or Page

a Web site or page no longer in use but subject to records retention plans.

Equal Opportunity Officer

For purposes of this policy, this role is filled for each campus by the following individuals:

- Fort Wayne: Equal Opportunity/Affirmative Action Officer
- Calumet: Director for Equal Employment Opportunity/Diversity
- North Central: Equal Opportunity/Affirmative Action Officer and Special Assistant to the Chancellor
- West Lafayette: Director, Office of Institutional Equity

Legacy Web Page

A Web page published prior to the effective date of this policy.

Redesigned Web Page

A Web page where significant alteration or update is made to the visual design of a page or a major revision of the content of a page takes place.

Sanctions

Additional Contacts

* References

"9.6 Policy on Student Computer Ownership." *Illinois State University*. N.p., n.d. Web. 10 Sept. 2014. <http://policy.illinoisstate.edu/technology/9-6.shtml>.

"E-Discovery Guideline and Toolkit." *EDUCAUSE Homepage*. N.p., n.d. Web. 10 Sept. 2014. <http://www.educause.edu/wiki/e-discovery-guideline-and-toolkit>.

"E-Discovery Policy." *Denison University*. N.p., n.d. Web. 10 Sept. 2014. <http://denison.edu/forms/e-discovery-policy>.

"Harvard Research Data Security Policy (HRDSP)." *Office of the Vice Provost for Research, Harvard University*. N.p., n.d. Web. 10 Sept. 2014. <http://vpr.harvard.edu/pages/harvard-research-data-security-policy>.

"Lamar University." *Accessibility Policy* -. N.p., n.d. Web. 10 Sept. 2014. <http://www.lamar.edu/about-lu/accessibility.html>.

"University Policies." *Security of Information Technology Resources: Information Technology (IT): Information & IT: Categories: Policies: Indiana University*. N.p., n.d. Web. 10 Sept. 2014. <http://policies.iu.edu/policies/categories/information-it/it/IT-12.shtml>.

"Web Accessibility." *Policy*. N.p., n.d. Web. 10 Sept. 2014. <http://www.purdue.edu/webaccessibility/policy/>.

CREDIT CARD PROCESSING & SECURITY POLICY. University of Miami, n.d. Web. <https://umshare.miami.edu/web/wda/policiesfinance/eefiles/e071_credit_card_processing_security_policy.pdf>.