



Office of Internal Audit

**Audit of Internal Controls and Data Security
over Personal Data Pursuant to Florida
Department of Highway Safety and Motor
Vehicles Contract Number HSMV-0910-16
Report No. 19/20-02
August 26, 2019**

Date: August 26, 2019

To: Vanessa Merine, Director, Office of Admissions Operations, Enrollment Processing Services Department

From: Trevor L. Williams, Chief Audit Executive

**Subject: Audit of Internal Controls and Data Security over Personal Data
Pursuant to Florida Department of Highway Safety and Motor Vehicles
Contract Number HSMV-0910-16 – Report No. 19/20-02**



Pursuant to your request, we performed an audit of the internal controls and data security governing the Office of Admissions Operations, Enrollment Processing Services department's use and dissemination of personal data pursuant to the requirements of the Florida Department of Highway Safety and Motor Vehicles (DHSMV) Contract Number HSMV-0910-16. The objectives of the audit were to determine whether the Enrollment Processing Services department has policies and procedures in place to prevent unauthorized access, distribution, use, modification, or disclosure of the personal data provided or received pursuant to the executed memorandum of understanding.

You will note that the scope and breadth of the current audit is more expansive than that of similar audits of the driver license and motor vehicle data received under prior DHSMV contracts, due to the new audit requirements stipulated in the current contract. Consequently, these new requirements have impacted the reporting format and results of our audit.

The audit also forms a basis for us to sign the Florida Highway Safety and Motor Vehicles Attestation Statement certifying that we have evaluated the internal controls over personal data and that the controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure; and to certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence.

We want to take this opportunity to express our appreciation to you and your staff for the cooperation and courtesies extended to us during the audit.

Attachment

C: Board of Trustees

Mark B. Rosenberg, University President

Kenneth G. Furton, Provost, Executive Vice President and Chief Operating Officer

Kenneth A. Jessell, Chief Financial Officer and Senior Vice President

Javier I. Marques, Vice President and Chief of Staff, Office of the President

Kevin B. Coughlin Jr. Vice President Enrollment Services

Robert N. Grillo, Vice President and CIO

TABLE OF CONTENTS

	<u>Page</u>
SCOPE, OBJECTIVES, METHODOLOGY, MANAGEMENT'S RESPONSIBILITY, AND AUDITOR'S RESPONSIBILITY.....	1
1. Audit Scope and Objectives.....	1
2. Audit Methodology.....	1
3. Management's Responsibility.....	2
4. Auditor's Responsibility.....	2
BACKGROUND	2
OVERALL SUMMARY AND INTERNAL CONTROL RATING	3
1. Section I – Summary of Audit Results and Management's Corrective Actions	4
2. Section II – Florida Highway Safety and Motor Vehicles Attestation Statement.....	21
GLOSSARY OF ABBREVIATIONS	23

SCOPE, OBJECTIVES, METHODOLOGY, MANAGEMENT'S RESPONSIBILITY, AND AUDITOR'S RESPONSIBILITY

Audit Scope and Objectives

We performed an audit of the Office of Admissions Operations, Enrollment Processing Services Department's ("EPS" or "the EPS Department") internal controls and data security governing the use and dissemination of personal data pursuant to the requirements of the Florida Department of Highway Safety and Motor Vehicles (DHSMV) Contract Number HSMV-0910-16 ("MOU"). According to Section VI, Part B, of the MOU, the agreement is contingent upon the EPS Department having appropriate internal controls over personal data. In furtherance of this requirement, the DHSMV requested FIU to submit an attestation from either a certified public accounting firm or its internal auditor.

The objectives of the audit were to determine whether the EPS Department has policies and procedures in place to prevent unauthorized access, distribution, use, modification, or disclosure of the personal data that is provided or received pursuant to the MOU.

Audit Methodology

The audit methodology was based on the requirements of the MOU and the DHSMV External Information Security Policy. To align with the requirements of the MOU, our audit included evaluation of internal controls in place during the MOU service year ended May 31, 2019. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and ISACA *IS Audit and Assurance Standards* and included tests of the applicable standards identified in DHSMV External Information Security Policy and such other auditing procedures, as we considered necessary under the circumstances. We performed our audit fieldwork between June and August 2019.

To satisfy our objectives, we:

- Reviewed University policies and procedures, applicable Florida Statutes, MOU HSMV-0910-16, and the DHSMV External Information Security Policy;
- Observed the EPS Department's current processes and practices;
- Interviewed responsible personnel; and
- Tested selected relevant controls.

The controls tested, the results of the tests, and management's corrective actions, where applicable, are presented in Section I – Summary of Audit Results and Management's Corrective Actions.

The University's Information Technology Department ("Division of IT" or "DoIT") completed a risk assessment of the EPS Department and was instrumental in assisting the EPS Department with identifying and remediating security vulnerabilities identified through the risk assessment. The Division of IT also assisted the EPS Department with correcting

deficiencies identified during the audit. In conducting the audit, we relied on the work performed by the Division of IT to satisfy the testing of certain audit objectives.

Management's Responsibility

Pursuant to the MOU, the Office of Admissions Operations, Enrollment Processing Services is responsible for ensuring that appropriate internal controls are in place at all times that data is being provided or received pursuant to the MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The Enrollment Processing Services' management is also responsible for ensuring that deficiencies found during the audit are corrected and measures are put in place to prevent recurrence.

Auditor's Responsibility

Our responsibility is to: (1) provide an Attestation Statement indicating that we have evaluated the internal controls over personal data and that the controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure; and (2) certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. Our audit forms a basis for us to sign the Florida Highway Safety and Motor Vehicles Attestation Statement on page 22.

BACKGROUND

Per Florida Statues Section 1009.21, students shall be classified as either Florida residents or nonresidents for tuition purposes. On May 19, 2016, Florida International University's (FIU) Enrollment Processing Services entered into the Memorandum of Understanding 0910-16 with the Florida Department of Highway Safety and Motor Vehicles. The MOU is a six-year agreement which allows the EPS electronic access to driver license and motor vehicle data, stored in the DHSMV's Driver and Vehicle Information Database (DAVID) system, to be used to verify information submitted for initial residency classification for tuition purposes as part of the admissions process at FIU. The agreement expires May 19, 2022, and its continuance is contingent upon the EPS having appropriate internal controls in place at all times to protect the data, that is being provided or received pursuant to the MOU, from unauthorized access, distribution, use, modification, or disclosure.

The MOU requires that EPS develop security requirements and standards consistent with the DHSMV External Information Security Policy (EISP) and employ adequate security measures to protect the information, applications, data, resources, and services. Although prior to the commencement of our audit the EPS Department had a documented 'Initial Residency Review Process' and employed certain control activities related to its use of DAVID, it lacked documented policies and procedures that provided guidance over its use of DAVID. During the course of the audit, the EPS Department codified its operating practices and controls pertaining to its use of DAVID into an operational manual. The newly developed policies are referenced in the table on pages 5 – 20.

OVERALL SUMMARY AND INTERNAL CONTROL RATING

Our audit concluded that Enrollment Processing Services' current policies and procedures are adequate to prevent unauthorized access, distribution, use, modification, or disclosure of the personal data that is provided or received pursuant to the MOU. However, during the audit, we identified opportunities to strengthen EPS' internal controls that pertain to data access security, Quarterly Quality Control Review (QQCR) documentation, timely review of vulnerability scans and Data Loss Prevention (DLP) reports, password protection, and segregation of duties. Measures to strengthen these areas of control were codified into a newly developed DAVID Operational Manual. Also, prior to the conclusion of this audit, the EPS Department corrected the deficiencies identified and enacted measures to prevent recurrence. Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	SATISFACTORY	FAIR	INADEQUATE
Process Controls	X		
Policy & Procedures Compliance	X		
Effect	X		
Information Risk	X		
External Risk	X		

INTERNAL CONTROLS LEGEND			
CRITERIA	SATISFACTORY	FAIR	INADEQUATE
Process Controls	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance	Non-compliance issues are minor	Non-compliance Issues may be systemic	Non-compliance issues are pervasive, significant, or have severe consequences
Effect	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk	Information systems are reliable	Data systems are mostly accurate but can be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Potential for damage	Severe risk of damage

SECTION I – SUMMARY OF AUDIT RESULTS AND MANAGEMENT’S CORRECTIVE ACTIONS

The areas tested during the audit, our observations, and management’s corrective actions related to the internal processes in place to protect the data as outlined in the MOU and the DHSMV’s EISP are presented on pages 5 through 20.

The following table summarizes our testing and conclusions, and describes: (1) the DHSMV External Information Security Policy, which all agents, vendors, contractors and consultants (External Entities) who use and/or have access to the DHSMV information resources must adhere to; (2) the requirements outlined in the MOU HSMV-0910-16; (3) FIU and EPS policies, procedures, and processes that are applicable to the MOU; (4) our audit objectives and procedures; and (5) our audit observations and corrective actions taken, where applicable. The EPS policies included in the following table were developed during the course of the audit.

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS				
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken
#A-02: Data Security	MOU Section V – Safeguarding Information, Part H	FIU Policy 1930.020b IT Security Procedure: Sharing Access to IT Resources; Password Management	<p>Audit Objectives: Determine if persons granted access to DAVID were employees of EPS and if the access granted were based on their roles and responsibilities at the EPS Department.</p> <p>Audit Procedures: Obtain a list of all employees' granted access to DAVID and compare to the list of all active employees in the EPS Department for the audit period to determine if all persons with access to DAVID are active employees of the EPS Department.</p>	<p>No exception noted – All active users of the DAVID system are current full-time employees of FIU's Enrollment Processing Services Department, whose job duties are related to residency verification.</p> <p>Review the job descriptions in PantherSoft for all employees with access to DAVID to ascertain if their roles and responsibilities includes verification of initial residency for admissions.</p> <p>Confirm job function of each employee with the EPS</p>

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS				
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken
		<p>business transactions with the University. Limiting access to IT resources by using access codes enables the University to better monitor and control usage of its resources. In the case of PantherSoft, moreover, controlling access precludes individuals from being able to view system data and records to which they should not be privy, and it precludes individuals from initiating transactions which they are not authorized to perform.</p>	<p>Department's director to determine that user access is appropriate.</p>	<p>No exception noted – All active user accounts created in the DAVID system by EPS had uniquely identified user ID and were linked to current full-time employees of the EPS Department. We did not uncover any generic accounts in EPS. In addition, the roles assigned to each user were those necessary for residency verification.</p>
#A-02: Data Security	MOU Sections V – Safeguarding Information, Parts A and H	<p>FIU Enrollment Services Procedures</p> <p>The Director of Enrollment grants access to employees based on their job duties for verification of initial residency for admissions purposes. Staff will only access DAVID during specified work hours set by the POC [Point-of-Contact] and will only access DAVID for purposes of verifying information related to the Initial Florida Residency review. Searchers are only allowed under the Residency Verification Search Purpose code 026, which is set up as the 'DEFAULT' search code for all AO [Admissions Operations] staff.</p> <p>(A) Information exchanged will not be used for any purposes not specifically authorized by this MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, or the dissemination, sharing, copying, or passing of this information to unauthorized persons.</p> <p>(H) DAVID access shall be provided to users who are direct employees of the Requesting Party.</p>	<p>Audit Objectives: Determine if all users with access to DAVID have a uniquely identified login profile and if generic/administrative accounts were created.</p> <p>Audit Procedures: Obtain a list of all accounts created in DAVID for the EPS Department and ensure that they are all uniquely identifiable to an active full-time employee. Review the assigned roles for each employee listed and determine if the user was assigned only roles that are required for purposes of verifying residency, such as 'search motor vehicles by make and model', 'search/view driver's license records,' and 'last four social security numbers.'</p>	<p>Observations:</p>

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
#A-02: Data Security 4.0 Data Storage or Transmission	MOU Section V – Safeguarding Information, Part C	User account is created for each employee who is granted access to DAVID.	Audit Objectives: Determine if confidential or sensitive data transmitted or stored by EPS is secure. Audit Procedures: Obtain an understanding of the type of data EPS transfers and/or stores on its computer systems or in manual files. Review the security protocols and mechanisms, including encryption and lockdown tools in place to protect such data. Ensure that audit log files downloaded for the Quarterly Quality Control Review (QQCR) are secure and the encryption technology use aligns with the DHSMV's requirements.	Observations: <u>Exception noted –</u> Downloaded DAVID audit log data, which includes sensitive information, were saved in a folder on the EPS Department's Network drive, which is accessible by all the EPS Department's employees. <u>Corrective Actions Taken –</u> With assistance from the DoIT, EPS set up a secure folder with restricted access only to the Director and Associate Director on its 256-bit encrypted SharePoint drive. Audit log files will be moved from the Network folder to the restricted folder and future log files will be stored in the restricted folder. The SharePoint encryption technology is compliant with the DHSMV's requirements.	
#A-02: Data Security 5.0 Data Disposal	MOU Section V – Safeguarding Information, Part E	When printed information from DAVID is no longer needed, it shall be destroyed by cross-cut shredding or incineration.	Audit Objectives: Determine if confidential or sensitive data transmitted or stored by the EPS Department is properly disposed after authorized use.	Observations: <u>No exception noted –</u> EPS does not print sensitive DAVID-related information and only downloads DAVID audit log data. (Refer to our observations and	

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHS/MV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
explicit access rights. External Entities shall follow an established process approved by the Department for the disposal of data to include the disposal of confidential data in accordance with The Florida Public Records Act and Federal Standards.	documents are properly destroyed, only cross-cut or micro-cut shredders will be used to shred hardcopy records containing sensitive information. <u>Storage Media Destruction -</u> Destruction of sensitive information captured on computer storage media must only be performed by the Information Security Department.	Audit Procedures: Obtain an understanding of the type of data EPS prints or stores. Ascertain how such data is destroyed and review record of destruction, such as manifest and log.	Audit Procedures: Determine if appropriate EPS personnel receives, reviews, and maintains logs and audit trails of DAVID access/use.	Management's corrective actions detailed in section #A-02: Data Security, 4.0 Data Storage or Transmission above.) Also, the EPS did not dispose of any computers during the audit period.	
#A-02: Data Security	MOU Section II – Definitions, Part K	FIU Enrollment Services Procedures	Audit Objectives: Determine if appropriate EPS personnel receives, reviews, and maintains logs and audit trails of DAVID access/use.	Observations: <u>Exception noted –</u> Our audit determined that DAVID audit log data was downloaded for review and the QCRR were completed as evidence of the review occurrence. However, we were unable to determine if the reviews were completed within 10 days after the end of the quarter and the specific elements reviewed, due to the audit trails for the reviews not being sufficiently documented.	
6.0 Management Responsibilities	The Point of Contact (POC) is required to complete a Quarterly Quality Control Review Report each quarter to monitor compliance with this agreement. The following must be included in the Quarterly Quality Control Review Report: 1. A comparison of the DAVID users by agency report with the agency user list; 2. A listing of any new or inactivated users since the last quarterly quality control review; and 3. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination.	Per the MOU, the POC will run quarterly quality control audit logs, save them in a secure SharePoint folder, and review the user activity logs for instances of misuse or security breaches. Additionally, a designated Admissions Operations staff member will review the weekly DLP reports received from the Information Security Office for inconsistencies or discrepancies in access and attempts to move sensitive information (to external drives for example). Inconsistencies identified will be investigated to determine their source and severity.	Audit Procedures: Obtain samples of Data Loss Prevention (DLP) reports and audit logs maintained by EPS and examine them for evidence of review by EPS personnel. Compare the results from the audit log review to the Quarterly Quality Control Review Reports (QCRR).	In addition, although the DAVID-generated audit log data captured most of the users' system activity, it did not capture the printing of DAVID-related data by a user. This appears to be a gap in the DAVID system that should be	
		Quarterly Quality Control Review Report - Must be			

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHSMV External Information Security Policy (EPS)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
	completed, utilizing Attachment II, Quarterly Quality Control Review Report, within 10 days after the end of each quarter and maintained for two years.			<p>Corrective Actions Taken –</p> <p>The Director now maintains documentation of the user accounts and specific elements reviewed, and the test results. Additionally, EPS staff now receives and reviews the DLP report.</p> <p>Also, we recommended that the Director of EPS contact the DHSMV and inform them about the apparent gap discovered. In the interim, the Director has codified the EPS Department's operating practices into a DAVID Operational Manual, wherein EPS staff members are instructed not to print DAVID-related information.</p>	<p>Matter Resolved</p>
#A-02: Data Security	MOU Attachment I	FIU Policy 1930.020a Data Stewardship	Audit Objectives: Determine if the classification of data has been established by EPS and is consistent with the DHSMV's definitions.	<p>Observations:</p> <p>No exception noted –</p> <p>Our test confirmed that the data classifications delineated in FIU's Data Stewardship policy</p>	

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
Department. Data classification shall be done in accordance with Federal Information Processing Standards (FIPS) Publication 199 and is necessary to enable the allocation of resources for the protection of data assets, as well as determining the potential loss or damage from the corruption, loss, or disclosure of data. To ensure the security and integrity of all data, any data asset is Public, Sensitive or Confidential and should be labeled accordingly.	contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle record includes, but is not limited to, an individual's social security number, driver license or identification number, name, address, telephone number, medical or disability information, and emergency contact information.	disclosure by state or federal law, or by binding contractual arrangement. Among the types of data included in this category are individually identifiable financial or health information, social security numbers, credit card information, student education records and proprietary data protected by law or agreement.	Audit Procedures: Obtain and review FIU policy and compare it to the DHSMV's data classification requirements for alignment. Additionally, obtain and review evidence of staff's awareness of the classification of data, such as signed affidavit attesting to the review of the policy and record of training.	Exception noted – DAVID is a web-based application, and EPS accesses it using an Internet browser. DAVID's login password parameters are set and managed by the DHSMV. Therefore, we found no exception with EPS users' login credentials. However, for the workstations tested, DAVID timed out at 30 minutes. Windows screensaver timed out at varying intervals between 10 and 30 minutes, and some users stored their login credentials on their login screen.	
#A-04: Passwords	2.0 Policy and Standards	FIU Policy 1930.020b IT Security Procedure: Sharing Access to IT Resources; Password Management		Audit Objectives: Determine if user password convention is of sufficient strength, complexity, and constraints in accordance with the DHSMV requirements.	Audit Procedures: Obtain an understanding of the password convention established for EPS users of DAVID and compare it to the DHSMV password requirement for appropriateness.
All user accounts used to access the Department information resources shall have passwords of sufficient strength and complexity, and be implemented based on system requirements and constraints, and in accordance with the following rules to ensure strong passwords are established: <ul style="list-style-type: none">• expiration: 90 days.• length: 8 or more characters• complexity: enabled a combination of alpha (upper and lower case), numeric, and special characters (unless a particular system does not allow, passwords					

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	Corrective Actions Taken
shall consist of at least 3 of the above 4 categories). • history: last 10 passwords		<ul style="list-style-type: none"> history: last 5 passwords Multi-factor authentication is enforced via VPN. <p>FIU Enrollment Processing Services Procedures</p> <p>All users' DAVID passwords must comply with the requirements of EISP.</p>		<p>The Director of EPS immediately instructed all users to reset their workstation Windows screen timeout to ten minutes and instructed the identified users to remove the stored password and to discontinue this practice. EPS' new DAVID Operational Manual also mandates staff to log out of DAVID when away from their workstation.</p>	<p><u>Matter Resolved</u></p>
Computing devices shall not be left unattended without enabling a password-protected screensaver that is activated after 15 minutes of inactivity, or logging off the device. User accounts must be locked after 5 unsuccessful login attempts.					
#B-01: Acceptable Encryption		FIU IT Security Plan	<p>Audit Objectives: Determine if encryption technology is employed, as appropriate, and whether that technology meets the requirements of the DHSMV.</p> <p>Audit Procedures: Obtain a report from the DoIT detailing the encryption technology, include length of encryption key used to encrypt the EPS SharePoint drive on which audit logs are stored and compare it to the DHSMV's encryption requirements for appropriateness.</p>	<p>Observations:</p> <p>No exception noted – Our test confirmed that the encryption technology employed by the EPS' SharePoint drive where audit logs are stored complies with the DHSMV's encryption requirements.</p>	
4.0 Policy Encryption is the primary means for providing confidentiality for information that can be stored or transmitted, either physically or logically. When possible, confidential information should not be transmitted via email. If confidential information must be sent via email, it shall be encrypted. Information resources that stores or transmits sensitive or confidential data must have the capability to encrypt information. Proven, standard algorithms must be used as the basis for encryption technologies. Encryption key					

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
lengths must be at least 128 bits. The Department key length requirements will be reviewed periodically and upgraded as technology, legislation, or business needs requires.					
#B-02: Access Control		FIU Enrollment Processing Services Procedures	<p>Audit Objectives: Determine if all users with access to DAVID have a uniquely identified login profile, access was properly requested for all users, and if generic/administrative accounts were created.</p> <p>Audit Procedures: Obtain a list of all accounts created in DAVID for the EPS Department and ensure that they are all uniquely identifiable to an active full-time employee and the appropriate request to establish an account was made and approved prior to granting access to DAVID.</p>	<p>Observations:</p> <p>No exception noted – All active user accounts created in the DAVID system by EPS had uniquely identified user ID and were linked to current full-time employees of EPS. Each user account was created through the expressed authority granted in the executed MOU. In addition, we did not uncover any generic accounts in EPS.</p>	
2.0 Policy		Each full-time FIU employee with the Office of Admissions Operations whose job duties relate to residency verification is set up with a DAVID user ID and temporary password, which they must subsequently change upon initial login to DAVID.			
#B-02: Access Control		FIU Enrollment Processing Services Procedures	<p>Audit Objectives: Determine if users' access to DAVID is promptly disabled upon the occurrence of triggering events.</p> <p>Audit Procedures: Obtain a list of all user accounts created in DAVID during the audit period and a list of current account holders. Compare the two lists and investigate any differences to</p>	<p>Observations:</p> <p>No exception noted – No EPS employee was terminated or had a triggering event during the audit period that would necessitate disabling or removing a user's access in the DAVID system.</p>	
2.0 Policy		The Requesting Party agrees to immediately deactivate user access/permissions following termination or the determination of negligent, improper, or unauthorized use or dissemination of information.			
		A user's access shall be promptly disabled and/or removed from systems which access Department information resources, when access is no longer required. Examples include, but are not limited to, termination, transfer, or removal of the duties that require access. Notification of			

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHS/MV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
changes in the status of users with established Department credentials is the responsibility of the authorizing External Entity to report such changes to the Department.	reassignment of users within five (5) business work days.	Change in duties or responsibilities related to DAVID access. The POC will document the reason for the change in access, and the date the change is made.	determine whether accounts were disabled promptly. Perform test in conjunction with the test of user job duties and roles assigned to ensure that users whose job duties have changed have been removed from DAVID.	<u>Observations:</u> Exception noted – Our test disclosed that one of the three new users granted access to DAVID during the audit period did not sign the DAVID Acknowledgement form until the day after given access to DAVID.	
#B-02: Access Control		FIU Enrollment Processing Services Procedures Employee must sign the DAVID Legal Disclaimer in order to be provided access to DAVID.	<u>Audit Objectives:</u> Determine if DAVID account holders completed the appropriate written attestation prior to being granted access to DAVID. <u>Audit Procedures:</u> Obtain a list of all accounts created in DAVID for the EPS Department and ensure that the appropriate written acknowledgement was executed prior to being granted access to DAVID.	<u>Corrective Actions Taken –</u> EPS has developed operating procedures to formalize the on-boarding process related to access to DAVID, wherein the employee must sign the DAVID Legal Disclaimer prior to being granted access to DAVID.	
#B-02: Access Control				<u>Observations:</u> No exception noted – The Director of EPS stated that she reviewed the access rights of each user during each QCQR. Our review of the DAVID Edit User reports	
		FIU Enrollment Processing Services Procedures In cases that warrant a modification to a User account, the POC will edit the User Role through the DAVID Admin portal accordingly. Below are instances that may warrant a	<u>Audit Objectives:</u> Determine if there is a documented process in place to periodically review and modify users' account upon the occurrence of triggering events. <u>Audit Procedures:</u>		

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
		<p>User Role modification: 1. Change of name; 2. Change in work schedule or timeframe for accessing DAVID; and 3. Change in duties or responsibilities related to DAVID access. The POC will document the reason for the change in access, and the date the change is made.</p>		Inquiry of EPS management if there is a process in place to periodically review and modify DAVID users' access due to changes in their job duties or relationships. Obtain the DAVID Edit User report for all user accounts and review them for updates to the user's access rights.	provided evidence of changes to user accounts.
#B-02: Access Control				<p>Audit Objectives: Determine if user access rights are appropriate, consistent with the least-privilege concept, and appropriately segregated and free of conflicting roles.</p> <p>Audit Procedures: Obtain a list of all accounts created in DAVID for the EPS Department and review the assigned roles of each user to ensure that access is appropriate and there is proper segregation of duties.</p>	<p>Observations:</p> <p>Exception noted – Our test disclosed that both the Director and Associate Director's accesses lacked the proper segregation of duties.</p> <p>Corrective Actions Taken – The Director of EPS satisfactorily resolved the conflicts in hers and the Associate Director's accesses.</p> <p>Matter Resolved</p>
#B-03: Account Management for User Accounts				<p>Audit Objectives: Determine if access to DAVID was properly requested for all users.</p> <p>Audit Procedures: Obtain a list of all accounts created in DAVID for the EPS Department and ensure that the appropriate request to establish an account was made</p>	<p>Observations:</p> <p>No exception noted – Each user account was created through the expressed authority granted in the executed MOU.</p>

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS						
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken		
#B-03: Account Management for User Accounts				Audit Objectives: Determine if DAVID account holders completed the required training prior to being granted access to DAVID.		
		FIU Enrollment Processing Services Procedures	Audit Procedures: Employee must complete DAVID security training and FIU required IT security Cybersecurity Awareness Training in order to be provided access to DAVID.	Observations: No exception noted – Our test confirmed that all employees given access to DAVID during the audit period completed the DAVID security training as required.		
#B-03: Account Management for User Accounts				Audit Objectives: Obtain a list of all accounts created in DAVID for the EPS Department. Request copies of documents (certificates, system logs, training materials and attendance roster) evidencing that the required training was completed prior to being granted access to DAVID.		
		FIU Enrollment Processing Services Procedures	Audit Procedures: All users' DAVID passwords must comply with the requirements of the EISP.	Observations: No exception noted – DAVID is a web-based application, and EPS accesses it using an Internet browser. DAVID's login password parameters, including expiration, are set and managed by the DHSMV and are therefore compliant.		
#B-03: Account Management for User Accounts				Audit Objectives: Determine if user password expiration complies with the DHSMV requirements.		
		FIU Enrollment Processing Services Procedures	Audit Procedures: Obtain an understanding of the password convention established for EPS users of DAVID and compare it to the DHSMV password requirement for appropriateness.	Observations: No exception noted – No EPS employee was on extended leave of 60 days or greater during the audit period.		
#B-03: Account Management for User Accounts				Audit Objectives: Determine if users' access to DAVID is promptly disabled for a user on extended leave.		
		FIU Enrollment Processing Services Procedures	Audit Procedures: In cases that warrant a modification to a User account, the POC will edit the User Role through the DAVID Admin portal accordingly. Below are instances that may warrant a	Observations: No exception noted – No EPS employee was on extended leave of 60 days or greater during the audit period.		

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS				
DHSMV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken
leave is defined as greater than 60 days.	User Role modification: 1. Change of name; 2. Change in work schedule or timeframe for accessing DAVID; and 3. Change in duties or responsibilities related to DAVID access. The POC will document the reason for the change in access, and the date the change is made.	list of current account holders. Compare the two lists and investigate any differences to determine whether accounts were disabled promptly. Inquiry of EPS management if any DAVID user was on extended leave of greater than 60 days during the audit period.		
#B03: Account Management for User Accounts	FIU Enrollment Processing Services Procedures	In cases that warrant a modification to a User account, the POC will edit the User Role through the DAVID Admin portal accordingly. Below are instances that may warrant a User Role modification: 1. Change of name; 2. Change in work schedule or timeframe for accessing DAVID; and 3. Change in duties or responsibilities related to DAVID access. The POC will document the reason for the change in access, and the date the change is made.	Audit Objectives: Determine if there is a documented process in place to periodically review and modify users' account upon the occurrence of triggering events. Audit Procedures: Inquiry of EPS management if there is a process in place to periodically review and modify DAVID users' access due to changes in their job duties or relationships. Obtain a list of all user accounts created in DAVID during the audit period and a list of current account holders. Compare the two lists and investigate any differences to determine whether accounts were disabled.	Observations: <u>No exception noted</u> – EPS has developed procedures for reviewing and modifying user accounts when warranted, based on the circumstances. No EPS employee was terminated during the audit period.

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHS/MV External Information Security Policy (EISP) Provider	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
#B-06: Application Service Provider 1.0 Purpose To define minimum security requirements for an Application Service Provider (ASP) to the Department. This policy applies to ASPs that are either being considered for use by the Department or its agent, or have already been selected for use.			Audit Objectives: Determine if EPS have contracted with an ASP for its DAVID operations. Audit Procedures: Evaluate the results from our understanding of the internal controls and walkthrough related to EPS' use of DAVID and identify all contracted vendors who provide services to EPS in relation to its use of DAVID.	Observations: No exception noted – Not applicable as EPS does not use an ASP in its use of the DAVID system.	
#B-10: Incident Handling (Security Incidents) 2.0 Policy Information security incidents are events involving the Department's information resources, systems, or data, whether suspected or proven, deliberate or inadvertent that threatens the confidentiality, integrity, and availability, of the Department's information resources. The reporting of incidents enables the Department to review the security controls and procedures; establish additional, appropriate corrective measures, if required, and reduce the likelihood of recurrence.	MOU Section VI – Compliance and Control Measures, Part D – Misuse of Personal Information –	FIU Enrollment Processing Services Procedures	Audit Objectives: Determine if an incident response plan is in place and functioning properly. Audit Procedures: Obtain EPS' procedures on the handling of known or suspected security incidents/breaches and review for alignment with the MOU and EISP. No security incident occurred during the audit period; therefore, we were unable to test the effectiveness of the plan's execution. Additionally, our review of selected audit log reports did not disclose any identified suspected security incidents.	Observations: No exception noted – Our audit determined that the incident response procedures contained in EPS' new DAVID Operational Manual aligned with the requirements of the MOU and EISP. No security incident occurred during the audit period; therefore, we were unable to test the effectiveness of the plan's execution. Additionally, our review of selected audit log reports did not disclose any identified suspected security incidents.	

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS				
DHS/MV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken
Service, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed that impacts or has the potential to impact the Department's information resources, the Department's Information Security Manager (ISM) must be notified immediately and the appropriate incident management procedures must be followed.				<p>Observations:</p> <p>No exception noted –</p> <p>Not applicable.</p>

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHS/MV External Information Security Policy (EPS)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
trusted partners' networks and environments. External Entities who access or utilize Department information resources are subject to independent audit review.				Observations: No exception noted – Not applicable. EPS does not have a network connection to DAVID. All searches are effectuated via an Internet connection and individual unique ID login.	
#B-23: Network Interconnectivity			Audit Objectives: Determine if EPS accesses DAVID through a network connect and if the network has the appropriate firewall protections and complies with Florida Administrative Code Rule 74-2. Audit Procedures: Evaluate the results from our understanding of the internal controls and walkthrough related to EPS' use of DAVID and how it accesses DAVID. Review network architecture and determine the firewall or firewall features in place.	All External Entities' network connections must meet the requirements of the Florida Information Resource Security Policies and Standards (Rule 74-2). Blanket access is prohibited and the principle of least privilege shall apply. Interconnectivity is limited to services, devices, and equipment needed.	

SUMMARY OF AUDIT RESULTS AND MANAGEMENT'S CORRECTIVE ACTIONS					
DHS/MV External Information Security Policy (EISP)	MOU HSMV-0910-16	FIU / EPS Policies, Procedures, or Processes	Audit Objectives and Procedures	Audit Observations and Corrective Actions Taken	
#B-24: Malware/Virus Protection		<p>Managed hosts joined to the Active Directory Domain are required to have the host security tools which include, anti-virus, host data loss prevention, whole disk encryption, and host intrusion prevention. These tools are pushed to the hosts via GPO policies once they are joined to the active directory domain. Host firewalls are configured via GPOs. Hosts are patched using SCCM.</p>	<p>Audit Objectives: Determine if EPS devices that access DAVID are equipped with the approved malware and virus protection.</p> <p>Audit Procedures: Request the DoIT to run a report on each device used by EPS to access DAVID to determine whether the FIU virus protection software is installed and active on the device. The report should also indicate whether the virus protection system was altered.</p>	<p>No exception noted – Our test disclosed that all of EPS' devices have the McAfee Antivirus agent installed and active. The EPS devices are compliant with the DHS/MV's malware/virus protection requirements.</p>	

SECTION II – Florida Highway Safety and Motor Vehicles Attestation Statement

Terry L. Rhodes
Executive Director



2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

ATTESTATION STATEMENT

Contract Number HSMV-0910-16

In accordance with Section VI., Part A, of the Memorandum of Understanding between Department of Highway Safety and Motor Vehicles and FL International University - Enrollment Processing Center (Requesting Agency), this MOU is contingent upon the Requesting Party having appropriate internal controls over personal data sold or used by the Requesting Party to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. Upon request from the Providing Agency, the Requesting Party must submit an attestation stating that a currently licensed Certified Public Accountant performed an audit in accordance with the American Institute of Certified Public Accountants (AICPA), "Statements on Standards for Attestation Engagement." In lieu of submitting the attestation from a currently licensed Certified Public Accountant, the Requesting Party may submit an alternate certification with pre-approval from the Department. In the event the Requesting Party is a governmental entity, the attestation may be provided by the entity's internal auditor or inspector general. The attestation must indicate that the internal controls over personal data have been evaluated and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The attestation must be received by the Providing Agency within 180 days of the written request. The Providing Agency may extend the time to submit attestation upon written request and for good cause shown by the Requesting Agency.

FL International University - Enrollment Processing Center (Requesting Agency) hereby attests that Requesting Agency has evaluated and has adequate controls in place to protect the personal data from unauthorized access, distribution, use and modification or disclosure and is in full compliance as required in the contractual agreement.

Signature of Authorized Official

Vanessa Merine

Printed Name

Director, Enrollment Operations

Title

August 23, 2019

Date

Florida International University

NAME OF AGENCY

Signature of Auditor

Trevor L. Williams, CPA

Printed Name

August 23, 2019

Date

GLOSSARY OF ABBREVIATIONS

AO:	Florida International University's Office of Admissions Operations
ASP:	Application Service Provider
DAVID:	The Florida Department of Highway Safety and Motor Vehicles' Driver and Vehicle Information Database system
DHSMV:	The Florida Department of Highway Safety and Motor Vehicles
DLP:	Data Loss Prevention
EISP:	The Florida Department of Highway Safety and Motor Vehicles' External Information Security Policy manual
EPS:	Florida International University's Enrollment Processing Services Department
ESM:	Enterprise Security Management Team
FIU:	Florida International University
GPO:	Group Policy Object. It refers to a collection of Group Policy configurations defined for a specific system.
IS:	Information Security
ISM:	Information Security Manager
IT:	Information Technology
MOU:	Memorandum of Understanding
POC:	Point of Contact
QCQR:	The Florida Department of Highway Safety and Motor Vehicles' Driver and Vehicle Information Database system Quarterly Quality Control Review
QCRR:	The Florida Department of Highway Safety and Motor Vehicles' Driver and Vehicle Information Database system Quarterly Quality Control Review Report
SCCM:	System Center Configuration Manager