FIU | FLORIDA INTERNATIONAL UNIVERSITY

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-0512-18

Report No. 18/19-08

May 7, 2019

FLORIDA
INTERNATIONAL
UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: May 7, 2019

To: Thomas Hartley, Assistant Vice President, Department of Parking, Sustainability & Transportation

From: Trevor Williams, Chief Audit Executive

Trevor Williams

Subject: Audit of Internal Controls and Data Security over Personal Data Pursuant to Florida Department of Highway Safety and Motor Vehicles Contract Number HSMV-0512-18, Report No. 18/19-08

Pursuant to your request, we performed an audit of the Department of Parking, Sustainability & Transportation's ("the Department" or "Parking") internal controls and data security governing the use of personal data as required by the Florida Department of Highway Safety and Motor Vehicles (DHSMV) Contract Number HSMV-0512-18. The objectives of the audit were to determine whether the Department's policies and procedures for protecting personal data are: (1) adequate and effective, (2) being adhered to, and (3) ensure that the confidentiality of the data is maintained and protected. This includes an evaluation of the controls in place to prevent unauthorized access, distribution, use, modification, or disclosure of the personal data.

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 certified that: (1) the data security policies and procedures have been approved by a Risk Management IT Security Professional, (2) all deficiencies and/or issues found during the audit have been corrected, and (3) corrective measures have been enacted by the Department to prevent recurrence. Therefore, we are satisfied that the current internal controls adequately protect personal data from unauthorized access, distribution, use, modification, or disclosure.

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 of Operations & Safety and Chief of Staff
Robert N. Grillo, Vice President and CIO

TABLE OF CONTENTS

SCOPE, OBJECTIVES, METHODOLOGY, AND OPINION

Audit Scope –

We performed an audit of the Department of Parking, Sustainability & Transportation's 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-0512-18 ("MOU"). The objectives of the audit were to determine whether the Department has policies and procedures in place to prevent unauthorized access, distribution, use, modification, or disclosure of the personal data that is provided/received pursuant to the MOU and whether those data security policies and procedures have been approved by a Risk Management IT Security Professional.

Historical Background –

An audit of Internal Controls over Personal Data Pursuant to Florida Department of Highway Safety and Motor Vehicles Contract Number HSMV-0576-15 (Report No. 16/17-12) was last conducted on April 20, 2017. The prior audit scope was limited to attesting to the 14 questions provided by the DHSMV, which focused specifically on the completion of quarterly reviews and security and confidentiality awareness training; the protection of the information exchanged; the updating of user access upon employee reassignment and/or termination or the discovery of improper use of the data; the discovery and reporting of improper use of any information obtained as a result of the MOU; and whether the transfer of any right, duties or obligations under the MOU occurred without the consent and approval of the DHSMV. The current MOU's (HSMV-0512-18) audit requirements are more comprehensive and broader in scope. Beginning with this contract, in addition to the matters previously attested to, Parking must now develop security requirements and standards consistent with the Florida Information Technology Security Act (Section 282.318, Florida Statutes), Florida Cybersecurity Standards (Florida Administrative Code 74-2), and the DHSMV policy. The Department must also employ adequate security measures to protect the information, applications, data, resources, and services related to its use of data received pursuant to the MOU. In addition, the DHSMV now requires that the Department's data security policies and procedures be approved by a Risk Management IT Security Professional.

Management's Responsibility –

The Department of Parking, Sustainability & Transportation is responsible for: (1) designing, implementing, and maintaining a system of internal controls, including policies and procedures for Department personnel to follow and data security policies and procedures to protect personal data; (2) ensuring that the data security policies and procedures reviewed and approved by a Risk Management IT Security Professional; and (3) ensuring that deficiencies found during the audit are corrected and measures are put in place to prevent recurrence. Pursuant to the MOU, the appropriate management personnel must sign the audit report along with the independent auditor. The required management certification is included in Section III – Management's Certification.

Auditor's Responsibility –

Our responsibility is to: (1) evaluate the internal controls, including policies and procedures, governing the use and dissemination of personal data pursuant to the MOU and applicable laws, and to express an opinion on the adequacy of those controls to protect personal data from unauthorized access, distribution, use, modification, or disclosure; (2) verify that a Risk Management IT Security Professional has approved the Department's data security policies and procedures; and (3) verify that deficiencies found during the audit have been corrected and measures enacted to prevent recurrence.

Audit Methodology –

The audit methodology was based on the requirements of the MOU, DHSMV External Information Security Policy, and Florida Administrative Code 74-2 (F.A.C. 74-2). To align with the requirements of the MOU, our audit included an evaluation of internal controls in place during the MOU service year ended February 27, 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.* Those standards require that we plan and perform our audit to obtain reasonable assurance to satisfy our audit objectives. Our audit also included tests of the five high-level functions identified in F.A.C. 74-2 and such other auditing procedures, as we considered necessary under the circumstances. We performed our audit fieldwork between February and March 2019.

To satisfy our objectives, we:

- Reviewed University policies and procedures, FIU Board of Trustees (BOT) and Florida Board of Governors (BOG) regulations, applicable Florida Statutes and Florida Administrative Code 74-2, MOU HSMV-0512-18, and DHSMV External Information Security Policy;
- Observed the Department's current processes and practices;
- Interviewed responsible personnel;
- Tested selected transactions;
- Examined the internal controls over the data exchange environment between the FIU NuPark system and the DHSMV (see diagram on page 5); and
- Reviewed the controls over the Microsoft Azure Hosting platform services identified in the recent Service Organization Controls report (SOC 2) preformed for that platform. The report covered the AICPA Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy throughout the period October 1, 2017, to September 30, 2018.

Sample size and transactions selected for testing were determined on a judgmental basis applying a non-statistical sampling methodology. The controls tested, the results of the tests, and management's corrective actions, where applicable, are presented in Section II – Summary of Audit Results and Corrective Actions.

The University's Information Technology Department ("Division of IT") was instrumental in assisting the Department with determining the criteria necessary to risk rate its inventory. The Division of IT also completed a risk assessment of the Department.

Auditor's Opinion and Certification –

In our opinion, based on our audit, in all material respects, the internal controls and data security governing the Department of Parking, Sustainability & Transportation's use and dissemination of personal data pursuant to the MOU and applicable laws, which if operating effectively, were those necessary to provide reasonable assurance that personal data is protected from unauthorized access, distribution, use, modification, or disclosure. Our audit also confirmed that a Risk Management IT Security Professional has approved the Department's data security policies and procedures. Additionally, we verified that management has corrected the deficiencies found during the audit and has implemented measures to prevent recurrence.

Trevor Williams

May 7, 2019

Office of Internal Audit
Florida International University
Miami, FL

BACKGROUND

On February 27, 2018, Florida International University Board of Trustees; on behalf of the Department, entered into the Memorandum of Understanding 0512-18 with the Florida Department of Highway Safety and Motor Vehicles. The MOU is a three-year agreement which allows the Department electronic access to driver license and motor vehicle data to be used to verify vehicle registration and ownership information for the purpose of issuing University parking permits and collecting fines related to citations. The agreement expires February 27, 2021 and its continuance is contingent upon the Department and its third party hosting environment (NuPark) 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.

On August 22, 2014, the University, on behalf of the Department, entered into a three-year software subscription agreement with NuPark LLC (vendor), to provide a parking management system. The agreement was renegotiated on October 9, 2017 for one year with annual renewal terms. Under the agreement the vendor and the Department worked together and developed the University parking management solutions system called FIU NuPark ("the system").

The system is a database-encrypted, fully hosted, cloud-based parking management system and has the following features:

- Secured real time license plate recognition (LPR) technology, which provides the Department focused enforcement solution that enables the use of virtual or traditional permits using vehicle based mobile LPR cameras. The LPR provides the Department an effective way to verify parking permits, confirm mobile or meter-payments, issue citations, identify scofflaws, and provide vehicle location information all in real-time. The LPR technology allows for management of the enforcement process from permit verification to citation reconciliation.
- User friendly, secure, e-commerce online permit purchasing portal, and a mobile iOS or Android application, giving customers the ability to purchase permits and manage their account from phones and/or computers. The system facilitates acceptance of multiple payment methods, such as credit, debit, and payroll deductions.
- A back office to facilitate the system management and customer status. Customer profiles may be reflected in the system as a VIP or individual with specific lot/garage/space privileges. This information is communicated in real-time to all aspects of the system allowing the field officers to have the most up-to-date status information and giving them the ability to take appropriate action in the field.
- Citations are issued electronically via email for vehicles identified in the system or printed and mailed for unidentified vehicles. A one-way interface with the DHSMV was created to acquire vehicle owner information for unidentified vehicles. The DHSMV data flow diagram is shown on the following page.

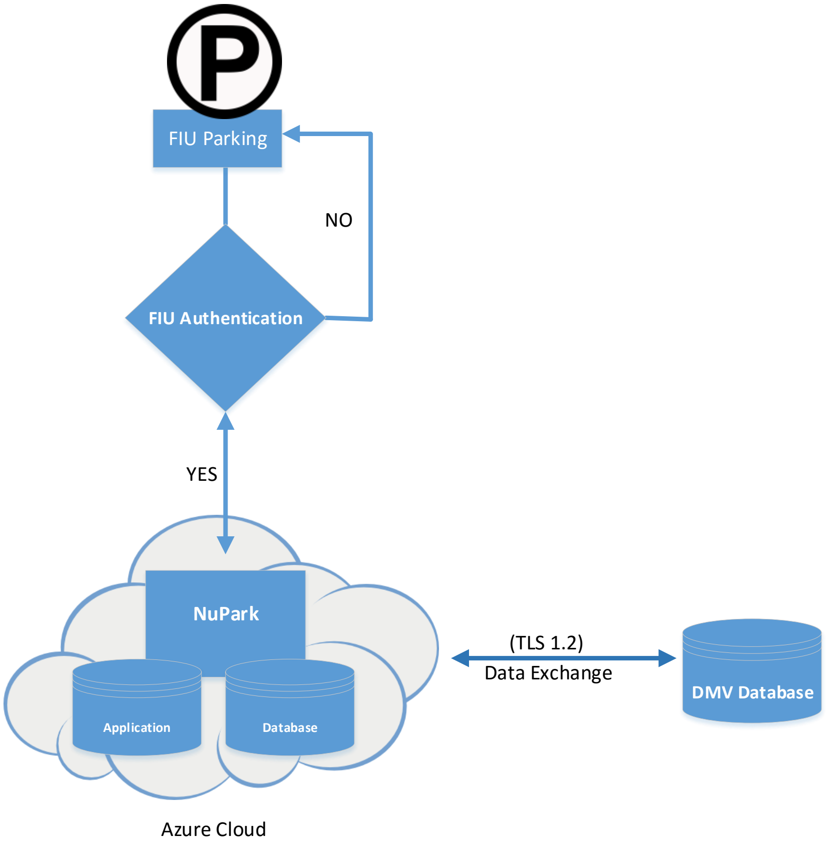

Figure 1 Data Process Flow Overview

The Department's users authenticate through the FIU Active Directory prior to accessing the NuPark System. Once connected, users are able to access citation information and also request data from the DMV database through a Transport Layered Security Version 1.2 encrypted data exchange connection.

The NuPark system is fully hosted in the Microsoft Azure platform. Microsoft is responsible for maintaining storage, security, operating system upgrades, routine maintenance, and the backup/recovery of the NuPark online system.

The Department's continued access to driver's license and motor vehicle data through the DHSMV is contingent on the Department's policies and procedures aligning with the requirements of Section 282.318, Florida Statutes (F.S. 282.318), Florida Administrative Code 74-2, and the DHSMV policy. As discussed in the section titled Objectives, Scope, Methodology and Opinion, this is a new requirement of the MOU. An overview of the scope of the F.S. 282.318, F.A.C. 74-2, and the DHSMV policy are as follows:

F.S. 282.318, *Security of data and information technology*, also known as the “Information Technology Security Act,” states that the Agency for State Technology is responsible for establishing standards and processes consistent with generally accepted best practices for information technology, including cybersecurity, to ensure availability, confidentiality, and integrity of an agency’s data to mitigate risks. The information security framework guidelines established by the act are consistent the Cybersecurity standards outlined in F.A.C. 74-2.

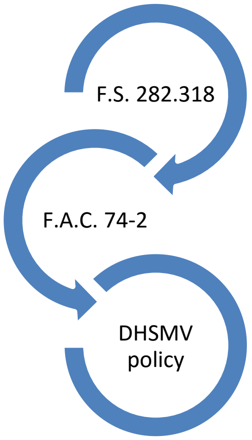

Figure 2 HSMV-0512-18

F.A.C. 74-2, also known as the Florida Cybersecurity Standards (FCS), establishes standards that State Agencies must comply with in the management and operation of their information technology (IT) resources. The FCS establishes minimum standards to be used by state agencies to secure IT resources. These standards consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risk. These functional activities should be evident in secure critical data residing on the FIU NuPark system.

The DHSMV policy applies to all agents, vendors, contractors, and consultants (External Entities) who use and/or have access to its information resources. External Entities who use and/or have access to the information resources shall adhere to the said policy. The authority for the DHSMV policy derives from F.S. 282.318 and F.A.C. 74-2.

OBSERVATIONS AND RECOMMENDATIONS

During the audit, we identified opportunities to strengthen the Department's internal controls that pertain to risk assessments, password parameters, timely reviews of vulnerability scans and DLP reports. Prior to the conclusion of this audit, the Department corrected the deficiencies identified and enacted measures to prevent recurrence. We have applied appropriate auditing procedures to verify the implementation and effectiveness of the corrective actions taken by management. 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 II – SUMMARY OF AUDIT RESULTS AND CORRECTIVE ACTIONS

The areas tested during the audit and our observations and recommendations related to the internal processes in place to protect the data as outlined in the F.A.C. 74-2 standards and the DHSMV policies are presented on the following pages.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Identity (ID)	**Asset Management (AM)**	***ID.AM-4*** Catalog interdependent external information systems.	***7.0 Data Classification*** The policy requires that data are classified in accordance with Federal Information Processing Standards (FIPS) Publication 199.	***FIU Policy #1910.005 Responsibilities for FIU Network and/or System Administrators*** The FIU Network and/or System Administrators are responsible for protecting the security and confidentiality of the data. The Administrator's responsibilities include, the purchase, implementation, maintenance, use, and disposition of IT resources.	***Data Security & Information Lifecycle Management, Classification*** According to the SOC 2 report, assets are classified in line with the Microsoft Online Classification Guidelines.	**Test Criteria:** Determine if the devices accessing and storing the data are assigned a classification based on data type, value, sensitivity, and criticality to the organization. **Audit Procedures:** Reviewed applicable FIU policies Reviewed Microsoft Azure SOC 2 report (vendor) Examined inventory list	**Observations:** **<u>Exception Noted</u> -** Parking did not maintain a current inventory list and the devices were not risk rated. **Corrective Actions Taken:** Parking updated the inventory list and risk rated the devices based on access to sensitive data. **<u>Matter resolved</u>**
		ID.AM-5: Prioritize IT resources based on classification, criticality, and business value.					
	Risk Assessment (RA)	***ID.RA-1:*** Identify and document asset vulnerabilities.	***#B-20: Security Monitoring and Auditing*** Per the policy, security monitoring is used as a method to confirm that security practices, controls, and policies are functional, adhered to, and are effective.	***FIU IT Security Plan*** The plan outlines that vulnerability scans are performed on a regular basis to all endpoints connected to the FIU network.	***Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection*** The SOC 2 report outlines that vulnerability scans and penetration tests are conducted monthly.	**Test Criteria:** Determine if procedures have been established to monitor the FIU NuPark environment for known security vulnerabilities and that the system is monitored for vulnerabilities as per documented procedures. **Audit Procedures:** Obtained and reviewed the processes in place to monitor the FIU NuPark environment for known security vulnerabilities. Determined whether the scans were completed and documented based on the established processes.	**Observations:** **<u>No exception noted</u> -** Vulnerability scans are completed by the Division of IT on a bi-weekly basis. Reports categorizing the results ranging from critical to non-critical are emailed to the IT Administrator, who is responsible for ensuring that vulnerabilities are remediated.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Identity (ID)	**Risk Assessment (RA)**	***ID.RA-3*:** Identify and document threats, both internal and external.	***#B-20: Security Monitoring and Auditing*** Monitoring should be instituted for Inbound and outbound traffic to/from External Entities, agents, and trusted partners' networks and environments.	***FIU IT Security Plan*** Vulnerability reports are shared with the various IT administrators for corrective action. Follow-ups and rescans are performed.	***Nupark Application and Data Security Policy*** The vulnerability scans and penetration tests reports are sent to the security team and Chief Technology Officer (CTO) for review and action.	**Test Criteria:** Determine if the results of vulnerability scans were reviewed and corrective actions taken. **Audit Procedure:** Selected a sample of devices from the risk rated inventory and performed testing, with Parking IT Administrator to ascertain that scan findings were tracked and remediated.	**Observations:** **<u>Exception Noted</u> -** Parking was not reviewing the scan reports and taking corrective actions in a timely manner. We reviewed the scan results for the audit period and identified a device with critical vulnerabilities which were repeated over an 11-month period without corrective actions being taken. This issue was also identified during the recently completed risk assessment by the Division of IT. **Corrective Actions Taken:** Parking management took immediate actions to correct the vulnerabilities identified during the audit and in the risk assessment report. Management informed us that going forward, the scan reports will be sent to the Director of Administrative Services and the IT Generalist. The Director will ensure that identified vulnerabilities are timely remediated. **<u>Matter resolved</u>**

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Identity (ID)	**Risk Assessment (RA)**	***ID.RA-4*:** Identify potential business impacts and likelihoods.	***#B-20: Security Monitoring and Auditing*** This policy defines the requirements and provides the authority for the Department's ISM, and Enterprise Security Management Team to conduct audits and risk assessments to ensure integrity of information resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.	***FIU Division of Information Technology*** FIU Chief Information Security Officer (CISO) completed a risk assessment of Parking Department risk rated device.	***Deloitte & Touche LLP*** A SOC 2 report was completed for the Microsoft Azure platform for the period October 1, 2017, - September 30, 2018.	**Test Criteria:** Determine if a risk assessment was completed, identified vulnerabilities were documented, and the risk responses were prioritized and corrections implemented **Audit Procedures:** Reviewed Parking's risk assessment completed by the Division of IT and the Azure SOC report to ascertain that the risk assessment procedures for identifying, assessing, and monitoring risks were established. As part of this process, threats to security are identified and risks from these threats are formally assessed and corrective actions implemented.	**Observations:** **<u>Exception Noted</u> -** Parking has not performed a risk assessment. **Corrective Actions Taken:** The University CISO performed a risk assessment of Parking's IT controls. The report identified 12 deficiencies, which were corrected by Parking. We reviewed updated supporting documentation and verified Parking took the appropriate corrective actions to remediate the risk assessment findings. **<u>Matter resolved</u>**
		ID.RA-5: Use threats, vulnerabilities, likelihoods, and impacts to determine risk.					
		ID.RA-6: Identify and prioritize risk responses.					

F.A.C. 74-2			**DHSMV ESP v2.0**	**FIU Controls**	**Vendor Controls**	**Test Criteria and Audit Procedures**	**Observations and Actions Taken**
Protect (PR)	**Identity Management and Access Control (AC)**	***PR.AC-1*:** Issue, manage, verify, revoke, and audit identities and credentials for authorized devices, processes, and users.	**#A-04*: Passwords*** Ensures the processes for creating, distributing, and changing, safeguarding, terminating, and recovering passwords adequately protect information resources. - expiration: 90 days - length: 8 or more characters - complexity: enabled - history: last 10 - multi-factor: No	***FIU Password Procedures*** User credentials must adhere to established standards and group policies for password requirements: - expiration:180 days - length: 8 or more characters - complexity: enabled - history: last 5 - multi-factor authentication is enforced via VPN.	***NuPark Password Procedures*** User credentials adhere to established standards and group policies for password requirements: - expiration: 90 days - length: 8 or more characters - complexity: enabled - history: last 4 Multi-factor authentication is enforced for production domains where passwords are not in use.	**Test Criteria:** Determine if policies and standards were established and implemented to enforce appropriate user account password expiration, length, complexity, and history. **Audit Procedures:** Examined Parking and the vendor's authentication password parameters and determined if they meet the DHSMV External Information Security Policy 2.0 requirements.	**Observations:** **Exception noted** - Parking password parameters, such as, history and expiration were not compliant with the DHSMV External Policy. **Corrective Actions Taken:** The Division of IT created two separate active directory groups, with the DHSMV required password parameters for the FIU NuPark users. **Matter resolved**
	Identity Management and Access Control (AC)	***PR.AC-4*:** Manage access permissions and authorizations, incorporate the principles of least privilege and separation of duties.	***#B-02: Access Control*** The Department utilizes the principle of least privilege for access control to information resources.	**FIU Policy #1930.020b, IT Security Procedures: Sharing Access to IT Resources** Access to University IT resources have been granted to students, faculty, and staff based on their roles and responsibilities at the University. This ensures that members of the University Community have access to only those resources necessary to perform their studies, job function, and/or business transactions with the University.	**Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection** Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege.	**Test Criteria:** Determine if Parking employs the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) that is necessary to accomplish assigned tasks in accordance with their roles. **Audit Procedures:** Matched the FIU NuPark user's vehicle privileges access, including those with administrator privileges, to the employee's job duties and determined if the access granted aligned with their duties.	**Observations:** **Exception noted** - The Office Coordinator's access to FIU NuPark was not aligned with her job duties. **Corrective Actions Taken:** Parking reduced the Office Coordinator's access to align with her duties. **Matter resolved**

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Protect (PR)	**Identity Management and Access Control (AC)**	***PR.AC-5:*** Protect network integrity, by incorporating network segregation and segmentation, where appropriate.	***#B-06: Application Service Provider*** The ASP must provide a proposed architecture document that includes a full network diagram of the Department Application Environment (initially provided to ASP by the Department), illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Department data resides, the applications that manipulate it, and the security thereof.	***FIU Network Diagram*** FIU CISO provided a data flow overview diagram documenting Parking's network segmentation through the use of firewalls.	***Identity & Access Management, Audit Tools Access*** Access segmentation to sessions and data in multi-tenant architectures by any third party is required.	**Test Criteria:** Determine if physical access mechanisms have been implemented and are administered to restrict access to authorized individuals. **Audit Procedures:** Examined Parking and the vendor's network controls to determine that the network is adequately segmented.	**Observation:** **No exception noted -** Our review of Parking and the vendor network controls disclosed that adequate controls were in place to ensure that the FIU NuPark network is appropriately segregated and segmented.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Protect (PR)	**Awareness & Training (AT)**	***PR.AT-1:*** Inform and train all users.	***#B-03: Account Management for User Accounts*** External Entities must complete Information Security Training on the Department's PartnerNet Portal within 30 days of receiving their account or risk having access terminated.	***FIU Division of Information Technology* (IT)** IT provides an online Security Awareness Training to educate employees on policies and procedures, standards, and information security practices to identify and prevent the loss of sensitive data. All employees are required to complete training prior to being granted access to the FIU NuPark system. Vendor employees with access to the FIU NuPark environment are required, by Parking, to review and sign the DHSMV's Driver and Vehicle Information Database system (DAVID) acknowledgement form documenting their understanding and acceptance of the sensitive nature of the data.	***Security Organization - Information Security Program*** An information security education and awareness program has been established that includes policy training and periodic security updates to Azure personnel.	**Test Criteria**: Determine if an information security education and awareness program was established and updated periodically. Determined that all users completed required training prior to access being granted as outlined in the MOU. **Audit Procedures:** Reviewed Parking procedures and determined that the training requirements noted in the MOU were documented. Selected a sample of employees granted access to FIU NuPark and determined that the required security awareness trainings were completed prior to access being granted.	**Observations:** **Exception noted -** The security training requirement was not documented in the Parking operating procedures manual. Five (5) of the 25 (20%) employees were granted access to the FIU NuPark system prior to their completion of the FIU Security Awareness Training. **Corrective Action Taken:** The Parking procedures manual was updated to reflect the FIU Security Awareness and/or DAVID training requirements. The identified employees immediately completed the FIU Security Awareness training. **Matter resolved**

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Protect (PR)	**Data Security (DS)**	***PR.DS-1:*** Protect data-at-rest.	***#B-01, Acceptable Encryption*** Information resources that stores or transacts 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 lengths must be at least 128 bits.	***FIU Policy #1930.020a Data Stewardship*** Highly Sensitive Data stored in electronic format must be encrypted using a minimum of 128 bit encryption. This applies to all local and shared drives.	***Common Criteria Related to Change Management*** Cryptographic controls are used for information protection within the Azure platform based on the Azure Cryptographic Policy and Key Management procedures.	**Test Criteria:** Determine if management processes and procedures, such as cryptographic keys used for encryption, which prevents unauthorized substitution, are in place and verified prior to encrypting data at rest, to prevent data loss. **Audit Procedures**: Obtained and reviewed Parking and the vendor's policies and procedures and determined if processes were established to manage cryptographic keys; for example, access controls are in place for secure key generation, and exchange and storage controls includes segregation of keys used for encrypted data or sessions.	**Observations:** **Exception noted -** Our test disclosed that both Parking and the vendor had adequate policies and procedures in place. However, we identified four devices for which the hard drives were not encrypted. **Corrective Actions Taken:** The Department worked with IT and implemented encryption on the devices identified. **Matter resolved**
		PR.DS-2: Protect data-in-transit.	**#B-01, Acceptable Encryption** Connections to the ASP utilizing the Internet must be protected using any of the following encryption technologies: IPsec, TLS, SSH/SCP, PGP, or any other encryption technologies approved by the Department's ISM.	***FIU Encryption*** FIU_NuPark.com site encryption is TLS 1.2.	***NuPark (Vendor) Encryption*** The server environment is encrypted with TLS 1.2.	**Test Criteria** Determine if the data received by Parking uses Transport Layer Security (TLS) version 1.2 or higher encryption. **Audit Procedures:** Obtained and reviewed screen prints for the FIU NuPark.com and the NuPark sites properties and determined if the connection encryption was TLS 1.2 or higher as required by the MOU.	**Observations:** **No exception noted -** Our review of the screen print confirmed that both sites currently have TLS 1.2 encryption.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Protect (PR)	Data Security (DS)	***PR.DS-5*:** Implement protections against data leaks or unauthorized data disclosures by establishing policies and procedures.	***#B-02: Access Control*** Each user accessing a Department information resource shall be assigned a unique personal identifier, commonly referred to as either a user account, login ID, user identification, or User ID. User access rights shall be established based on approved written requests. The user identification shall be traceable to the user for the lifetime of the records or reports in which they appear. Each user shall agree in writing to use the access only for the purpose intended.	***Parking, Sustainability and Transportation Procedures Manual*** All employees granted access to the data must complete the FIU Cybersecurity awareness training. Employees are also required to review and sign the DAVID online training data as acknowledgement of their understanding of the confidential nature of the data.	***Training and Awareness*** Information security training and awareness is provided to Azure employees, contractors, and third-parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Awareness training on security, availability, and confidentiality of information is provided to employees at the time of joining as part of induction.	**Test Criteria:** Determine if Parking established policies and procedures for the appropriate handling and protection of confidential information against data leaks or unauthorized data disclosures. Determine if employees were instructed on and acknowledged their understanding of, the confidential nature of the information. **Audit Procedures:** Obtained and reviewed Parking and the vendor's policies and procedures and determined controls in place to protect the data against leaks or unauthorized disclosure. Obtained the list of employees with access to the data. Selected a sample of employees and reviewed their training documentation to verify their understanding and acknowledgement of the policies and procedures and the confidential nature of the data being accessed.	**Observations:** **<u>No exceptions noted</u> -** Our audit found that Parking and the vendors policies and procedures outlined controls to ensure that the data was protected from leaks or unauthorized disclosure. Our test procedures confirmed that employees were instructed on the confidential nature of the data being accessed and acknowledged their understanding of the same.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Protect (PR)	**Information Protection Processes & Procedures (IP)**	***PR.IP-6:*** Destroy data according to policy.	***#A-02: Data Security 5.0 Data Disposal*** 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.	***FIU Media Sanitation Guidelines*** In order to protect University data, especially Highly Sensitive Data, from inadvertent or unauthorized use or disclosure, a University department or unit disposing of equipment with storage devices must ensure that the storage devices are erased using a repeated overwrite operation, purged, degaussed, or destroyed prior to storage media being sent to surplus, reused, donated, or discarded.	***Data Security & Information Lifecycle Management Classification*** The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements. Hard Disk Drive destruction guidelines have been established for the disposal of Hard Drives.	**Test Criteria:** Determine if Parking established policies and procedures to ensure that access to and disclosure of confidential information is restricted to authorized parties. Disposal of confidential information complies with the sanitation guidelines **Audit Procedures:** Obtained and reviewed Parking and the vendor's policies and procedures and determined if controls were in place to safeguard the data during removal, transfer, and disposition. Requested the list of equipment disposed by Parking during the audit period. Selected a sample of disposed equipment and confirmed if the sanitization process was performed.	**Observations:** **No exceptions noted -** During the audit we confirmed that Parking did not dispose of any equipment during the audit period.
		PR.IP-9: Establish and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery	***#B-10: Incident Handling (Security Incidents)*** Whenever a security incident, such as a virus, Denial of Service, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed that impacts or	**FIU Incident and Breach Response Policy** A Responding Party is designated by each unit and reports Privacy Breaches to FIU's Incident Response Team. The Responding	***NuPark Incident Management Policy*** The policy establishes and communicates a framework, with defined processes, roles, and responsibilities for	**Test Criteria:** Determine if an incident management framework has been established and communicated with defined processes, roles, and responsibilities for the detection, escalation, and response to incidents.	**Observations:** **No exceptions noted -** Our audit disclosed that the incident response time established by Parking and vendor complies with the MOU reporting requirements of 5 days.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Protect (PR)	**Information Protection Processes & Procedures (IP)**	and Disaster Recovery).	has the potential to impact the Department's information resources, the Department's ISM must be notified immediately and the appropriate incident management procedures must be followed.	Parties seek guidance in accordance with FIU's Incident Response Team. The Incident response reporting time is no more than 24 hours.	the detection, escalation, and response to security incidents. The vendor established an incident response time of 24 hours.	**Audit Procedures:** Reviewed Parking and vendor's incident response policies and procedures and determined if the response time aligns with the MOU requirements. Obtained and reviewed any security incident event reported during the audit period for timeliness	During the audit we confirmed that no data incident events were reported by Parking or the vendor.
		PR.IP-11: Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening).		***FIU Policy #1710.257 Background Check Requirements*** Level II criminal background screening are completed for positions with unrestricted access to information technology.	***Human Resources, Asset Returns*** Microsoft and NuPark personnel undergo formal screening, including background verification checks as a part of the hiring process prior to being granted access. Additional screening is conducted in accordance with customer specific requirements for employees with access to applicable data.	**Test Criteria:** Determine if level II background verification was completed for applicable Parking and vendor employees. **Audit Procedures:** Verified if level II background screening were completed for Parking and vendor employees with access to the data.	**Observations:** **<u>No exception noted</u> -** Our test confirmed that the required background screenings were completed for the applicable Parking and vendor employees.
	Protective Technology (PT)	***PR.PT-1***: Determine, document, implement, and review audit/log records in accordance with policy.	***#B-20: Security Monitoring and Auditing*** Security monitoring will be used as a method to confirm that security practices, controls, and policies are functional, adhered to, and are effective.	***Parking, Sustainability and Transportation Procedures Manual*** Quarterly reviews are completed of the FIU NuPark audit logs to detect and mitigate unauthorized activities.	***Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection*** Azure has established an Audit Log Management policy. Log and monitor access is	**Test Criteria:** Determine if Parking and the vendor perform internal reviews of the audit logs to detect and mitigate unauthorized activities. **Audit Procedures:** Obtained and inspected Parking quarterly reviews	**Observations:** **<u>No exception noted</u> -** Our test confirmed that Parking and the vendor have established policies and procedures for reviewing activity audit logs. Our review of the audit logs disclosed potential

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
					restricted to only authorized staff with a business need to access such systems.	and the vendor's SOC 2 report to ascertain if a review was performed and the results were reviewed with management.	inappropriate searches such as, SSN and DOB. Management confirmed that SSN and DOB data were not obtained
Detect (DE)	**Security Continuous Monitoring (CM)**	***DE.CM-1*:** Monitor the network to detect potential cybersecurity events.	***#B-23: Network Interconnectivity*** Ensure that interconnection of External Entities' networks to the Department's networks does not compromise the security of the Department's information resources.	***FIU IT Security Plan*** Vulnerability and data loss prevention (DLP) scans are performed to all endpoints connected to the FIU network. Network device patches are applied based on defined change management procedures. Notification of missing patches is done via the vulnerability reports, notifications, or assessments.	***Common Criteria Related to Monitoring of Controls*** Network device patches are evaluated and applied based on defined change management procedures.	**Test Criteria:** Determine if procedures have been established to monitor the network to detect potential cybersecurity events and to implement patches based on defined procedures. **Audit Procedures**: Selected a sample of devices with access to FIU NuPark, and obtained and inspected the DLP logs details to ascertain if vulnerabilities were assessed and remediated. Reviewed the SOC 2 report for the patch management process within the host environment (Microsoft Azure).	**Observations:** **Exception noted -** Our review determined that Parking was not reviewing the DLP reports and remediation actions were not timely taken. Our test of 23 devices showed that the DLP software was not installed on four (4) of the devices. We also noted that for one (1) device, the DLP report generated an alert for the possible transmission of personal identifiable data (PII). However, the alert was not timely investigated. **Corrective Actions Taken:** Parking worked with IT to ensure that all applicable vulnerability software were installed on the computers. The Director was added to the notification process to ensure that all vulnerability reports are reviewed and remediation actions are timely taken. The PII alert was subsequently investigated and it was determined that the data was not PII. **Matter resolved**

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Detect DE)	**Security Continuous Monitoring (CM)**	***DE.CM-3*:** Monitor personnel activity to detect potential cybersecurity events.	***#B-20: Security Monitoring and Auditing*** User access rights shall be established based on approved written requests. The user identification shall be traceable to the user for the lifetime of the records or reports in which they appear.	***Parking, Sustainability and Transportation Procedures Manual*** Parking management performs quarterly reviews of the user activities in FIU NuPark and all irregularities are investigated.	***Common Criteria Related to Monitoring of Controls*** A monitoring system has been implemented to monitor the Azure platform for potential malicious activity and intrusion past service trust boundaries.	**Test Criteria:** Determine if procedures have been established to monitor the personnel activity to detect potential unauthorized access and or searches. **Audit Procedures:** Obtained and reviewed Parking's personnel activity for the audit period. Identified and investigated any unusual activates identifies.	**Observations:** **Exception noted -** Our audit disclosed that searches were completed by two generic user accounts – "NuPark" and "Unknown". Management informed us that the searches were initiated by authorized users; however, due to a system glitch, the searches were not attached to the user's names. **Corrective Actions Taken:** Currently, Management reviews all searches initiated by the "NuPark" and "Unknown" accounts to determine which employee initiated the transactions. The vendor is developing a patch to address this issue. **Matter resolved**

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Detect (DE)	**Security Continuous Monitoring (CM)**	***DE.CM-4*:** Detect malicious code.	***#B-24: Malware/Virus Protection*** All computing devices (workstations, servers, laptops, tablets, etc.) whether connected to the Department's network or storing Department data, must utilize a Department approved virus protection system. The Department's ISM will maintain a list of approved protection vendors. Exceptions to this list will be considered for approval by the Department's ISM on a case-by-case basis.	***FIU Policy #1930.020c IT Security Procedure: System and Application Management*** All University-owned computing hosts that are subject to virus infection and are connected to the University network must have anti-virus software running, and anti-virus definition updates applied to them within 24 hours of their release.	***Common Criteria Related to Monitoring of Controls*** Procedures have been established to investigate and respond to the malicious events detected by the Azure monitoring system for timely resolution.	**Test Criteria:** Determine if devices with access to the data have supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template. **Audit Procedures:** Obtained and reviewed a list of the software installed on the risk rated devices and determined if antivirus software was installed and active on the devices.	**Observations:** **<u>Exception noted</u> -** Our test disclosed that four devices did not have the MacAfee antivirus agent installed. **Corrective Actions Taken:** Parking worked with IT and installed the McAfee antivirus and encryption on the devices. **<u>Matter resolved</u>**
		DE.CM-6: Monitor external service provider activity to detect potential cybersecurity events.	***#B-03: Account Management for User Accounts*** The Department reserves the right to audit the infrastructure utilized by the ASP to ensure compliance with this policy. Non-intrusive network audits (basic port scans, etc.) may be performed.	***Parking, Sustainability and Transportation Procedures Manual*** The NuPark Contract provides that Parking has the right to audit the contract and the right to receive the annual Microsoft Azure SOC 2 report.	***NuPark*** A SOC 2 report, which is completed annually for the Microsoft Azure platform is provided by the vendor to Parking.	**Test Criteria:** Determine if Parking receives and reviews the vendor's annual SOC 2 report and follows up on any unresolved findings related to the Azure hosting services. **Audit Procedures:** Inquired of Parking if they requested and reviewed the vendor's annual SOC 2 report. Determined if Parking has procedures in place to request, receive, and review the annual SOC 2 report and to document and follow up on any unresolved findings related to the Azure platform.	**Observations:** **<u>Exception noted</u> -** Our audit disclosed that Parking neither requested nor received the SOC 2 report from the vendor. Consequently, unresolved findings related to the host environment reported in the SOC 2 report had not been followed up on by Parking. **Corrective Actions Taken:** Management requested a copy of the vendor's current SOC 2 report for their review and amended their procedures manual to include a process of requesting and reviewing the vendor's SOC 2 reports. We reviewed the report and confirmed there were no unresolved findings related to the hosting environment.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
							Matter resolved
Detect (DE)	**Detection Processes (DP)**	***DE.DP-1:*** Define roles and responsibilities for detection to ensure accountability.	***#A-02: Data Security*** Network operations and systems administration personnel shall ensure that adequate logs and audit trails are maintained. Logs and audit trails must at a minimum record access to data, records, and activation of industry recognized security mechanism for protection of confidential and sensitive data.	***FIU IT Security Plan*** Vulnerability scans are performed on a regular basis to all endpoints connected to the FIU network. Vulnerability reports are shared with the various units' IT Administrators for corrective action. Follow-ups and rescans are performed.	***SOC 2 Report VM – 6*** Procedures have been established to monitor the Azure platform components for known security vulnerabilities.	**Test Criteria:** Determine if the roles and responsibilities for detecting anomalies are assigned to an employee. **Audit Procedures:** Obtained and reviewed the vulnerability scan distribution lists for the audit period and determined if the appropriate Parking employees were included. Interviewed the Parking employees to ascertain if they were informed of their roles and responsibilities for reviewing the scans.	**Observations:** **No exception noted -** The IT Generalist II in Parking is assigned the roles and responsibilities for reviewing the vulnerability scan results and ensuring corrective actions are taken.
Respond (RS)	**Response Planning (RP)**	***RS.RP-1:*** Execute response plan during or after an incident.	***#B-10: Incident Handling (Security Incidents)*** Ensure that computer security incidents which impacts, or has the potential to impact the confidentiality, integrity, and availability of the Department's information resources are properly recorded, communicated, and remediated.	***FIU Incident and Breach Response Policy*** The impact of any incident should be analyzed by the Responding Party in collaboration with the Incident Response Team.	***Common Criteria Related to System Operations*** An incident management framework has been established and communicated with defined processes, roles, and responsibilities for the detection, escalation, and response to incidents.	**Test Criteria:** Determine if Parking security incident response plan was operating according to policies. **Audit Procedures:** Obtained and reviewed the Parking's security incident response plan to ensure if it aligns with University and the MOU policies.	**Observations**: **No exception noted -** Our audit determined that Parking's security incident response plan was consistent with the MOU and the University's requirements. No security incident occurred during the audit period; therefore, we were unable to determine the effectiveness of the plan's execution.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Respond (RS)	Communications (CO)	***RS.CO-1*****:** Ensure that personnel know their roles and order of operations when a response is needed.	***#B-10: Incident Handling (Security Incidents)*** The DHSMV ISM must be notified immediately of any incident breaches.	***FIU Incident and Breach Response Policy*** The Incident Response Team should be notified as soon as possible, but no more than 24 hours after discovery of an incident that may have resulted in a privacy breach.	**NuPark** The vendor will notify Parking of incident breach within 24 hours of the incident.	**Test Criteria:** Determine if Parking personnel are aware of their roles and responsibilities in the event of a security incident breach. **Audit Procedures:** Obtained and reviewed Parking and the vendor's incident response policies and procedures and determine if a responsible party was assigned and informed of his/her roles and responsibilities pursuant to the policy.	**Observations:** **No exception noted -** Our audit confirmed that Parking established roles and responsibilities to ensure that notifications of breaches are received from employees and the vendor in sufficient time for them to notify the DMV and FIU CISO.
		RS.CO-5: Engage in voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness.		***FIU Division of IT*** The Division of IT is a member of several cybersecurity advisory boards and shared information received with the Parking IT Administrator.		**Test Criteria:** Determine if the University engages in voluntary information sharing with external stakeholders and discloses information received to various units, such as Parking. **Audit Procedures:** Obtained and reviewed documents to support if Parking's IT Administrator was notified of cybersecurity advisory information.	**Observations:** **No exception noted -** The Division of IT is a member of the MS-ISAC and the National Cyber Awareness System. Information garnered through FIU Division of IT's association with the MS-ISAC is shared with Parking's IT Administrator.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Recover (RC)	**Improvements (IM)**	**RC.IM-1**: Incorporate lessons learned in recovery plans.		***FIU Incident and Breach Response Policy*** The incident and breach response procedures will be tested and reviewed periodically. The test should include a walk-through of the plan components, the actions that would be taken in the test scenario(s), and a review of the test results to determine how the systems or processes should be improved. Improvements should also come from actual use and lessons learned.	***Business Continuity Management & Operational Resilience, Business Continuity Planning*** The Business Continuity Plans (BCP) team conducts testing of the Business Continuity and Disaster Recovery plans for critical services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.	**Test Criteria:** Determine if the vendor test the recovery plan and incorporate lessons learned into the plan. **Audit Procedures**: Obtained and reviewed the SOC 2 report prepared for the Microsoft Azure platform and determined that lessons learned from test were incorporated into the Azure Business Continuity Plan.	**Observations**: **<u>No exception noted</u> -** Our test disclosed that the vendors have procedures in place to ensure that data loss scenarios are tested annually and issues identified are resolved and updated accordingly.

F.A.C. 74-2			DHSMV ESP v2.0	FIU Controls	Vendor Controls	Test Criteria and Audit Procedures	Observations and Actions Taken
Recover (RC)	**Improvements (IM)**	**RC.IM-2:** Periodically update recovery strategies**.**		***FIU Incident and Breach Response Policy*** The incident and breach response procedures will be tested and reviewed periodically. The test should include a walk-through of the plan components, the actions that would be taken in the test scenario(s), and a review of the test results to determine how the systems or processes should be improved. Improvements should also come from actual use and lessons learned.	***Datacenter Business Continuity Management Program*** The program defines the business continuity planning and testing requirements for functions within the datacenters. Datacenters are required to at least annually, exercise, test, and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption.	**Test Criteria**: Determine if Parking has policies and procedures in place to periodically test, review, and update the incident response plan. **Audit Procedures:** Obtained and reviewed Parking and the vendor's security incident response plans. Determined if the plans were periodically reviewed, tested, and updated, based on lessons learned.	**Observations:** **<u>No exception noted</u> -** Our test confirmed that Parking and the vendor completed a review of their incident response plans. The plans were periodically reviewed, tested, and updated, based on lessons learned.

SECTION III – MANAGEMENT’S CERTIFICATION

FIU | Operations and Safety

FLORIDA INTERNATIONAL UNIVERSITY

TO: State of Florida

RE: HSMV-0512-18

DATE: May 7, 2019

To whom it may concern:

Pursuant to the requirements of the Florida Department of Highway Safety and Motor Vehicles (DHSMV) Contract Number HSMV-0512-18, we certify that:

1. Data security policies and procedures to protect personal data and to prevent unauthorized access, distribution, use, modification, or disclosure of such data have been implemented and maintained.

2. The data security policies and procedures reviewed and approved by a Risk Management IT Security Professional.

3. All deficiencies identified during the current audit of Contract Number HSMV-0512-18, which for the first time required the consideration of the provisions of certain laws and Agency policies, have been corrected and measures have been enacted to prevent recurrence.

Thank you.

APPROVED:

Javier I. Marqués,
Vice President for Operations & Safety
Chief of Staff

Thomas Hartley
Assistant Vice President, Parking,
Sustainability & Transportation

Approved as to form
and legality

F.I.U. Attorney

Definition of Internal Auditing

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.