MEMORANDUM

DATE: December 29, 2015

TO: CFX Board Members

FROM: Corey Quinn, Chief of Technology/Operations

COPIES: Darleen Mazzillo, Executive Assistant

SUBJECT: Security Policy Update

Board approval is requested for the attached redlined Security Policy update. The policy has been updated to reflect the Central Florida Expressway Authority name and minor administrative changes.

Central Florida Expressway Authority

Security Policy

Version 3.~~2~~1

~~March 25, 2014~~ January 14, 2016

AMENDMENT REGISTER

Version No	Version Date	Amendment Description	Amended By
1.0	August, 2004	Original Version	Neal Jones, MSXI
1.1	November, 2005	Added Updates Required for PCI compliance	Bill Brownsberger, MSXI
2.0	October, 2006	Added Streaming Video and Audio Restrictions	Joann Chizlett
2.1	December, 2006	Added Instant Messaging Restriction	Bill Brownsberger, MSXI
2.2	May, 2008	Added file sharing and torrent sites Restrictions	Joann Chizlett
2.3	October, 2009	Rewrite and Reformat	Rene Rodrigue
3.0	November, 2009	Draft to Final	IT / Finance Dept
N/A	October 2013	Reviewed for PCI DSS Compliance	Rene Rodrigue
3.1	March 2014	Added Facility Access Policy Portion	IT / HR
3.2	January 2016	Modified for CFX	Corey Quinn

I. Introduction to Information Security Policy

Computer information systems and communications networks are integral and critical parts of the Central Florida Expressway Authority's (~~Authority~~CFX) business operations. ~~The Authority~~CFX has made a substantial investment to establish and protect these systems and the misuse of information or systems can do irreparable harm to the Authority, its employees and customers. It is therefore vital that all ~~Authority~~ CFX staff and contractors commit to safeguarding these resources. Those who have access to ~~Authority~~ CFX data are to use the utmost care in its protection from unauthorized disclosure, alteration, destruction or publication. Anyone responsible for the willful and negligent handling of ~~the Authority~~CFX's systems, data or equipment shall be properly disciplined, up to and including termination and/or filing of a complaint with law enforcement.

~~The Authority~~CFX maintains many data files that are considered highly confidential from which negative consequences would ensue should the information be published or otherwise divulged negligently or maliciously. All confidential data must be treated as confidential with access limited to those whose access is required to perform their assigned duties. Staff is directed to implement security procedures that outline the care to be exercised by all employees and contractors related to ~~Authority~~ CFX systems and equipment. In all cases where the correct course of action is uncertain, employees should always seek guidance from their supervisor or human resources representative. Contractors should seek guidance from their immediate supervisor and/or ~~Authority~~ CFX contract point person.

~~The Authority~~CFX reserves the right, without notice or warning, at any time, to audit and / or monitor the use of ~~Authority~~ CFX systems, data and / or equipment for the purpose of ensuring compliance with this and other security related documents such as the 'Employee Security Guidelines Handbook' and 'Contractor Security Guidelines Handbook'.

II. Information Security Policy

A. All computer system data and customer information that is maintained by ~~the Authority~~CFX, whether electronic or hardcopy, is considered to be confidential unless specifically defined as open to the public.

B. All ~~Authority~~ CFX employees and contractors are required to obtain written permission to disclose ~~Authority~~ CFX information to anyone other than ~~Authority~~ CFX employees or contractors who need the information to conduct their official business. All other requests for information, except for inquiries from the media, shall be routed through ~~the Authority~~CFX's Records Custodian who will determine if information is legally public record prior to its release. If there is any doubt as to the information's legal status, General Counsel shall be consulted. Requests for information from the media shall be routed through the Marketing and Communications Department.

C. All employees and contractors must adhere at all times to the processes, procedures and guidelines as set forth in their respective 'Security Guidelines Handbook', i.e. the 'Employee Security Guidelines Handbook' or the 'Contractor Security Guidelines Handbook'. Failure to adhere with the provisions of these respective documents, as applicable to employee or contractor, could result in disciplinary action up to and including termination. Additionally, civil penalties and fines could also apply. The above documents are living documents and they will change from time to time in order to add, delete or modify processes, procedures and / or guidelines.

D. Employees and contractors will only use ~~Authority~~ CFX systems, information and equipment in a manner consistent with the employees and / or contractor's job function and requirements. ~~Authority~~ CFX resources are to be used for ~~Authority~~ CFX business only.

E. You may not access or disseminate material that is offensive, harassing or illegal (ex. software piracy) in nature, including but not limited to material that disparages others based on race, religion, ethnicity,

gender, sexual orientation, age, disability or political affiliation. In addition, you may not access or disseminate sexually explicit or sexually oriented messages, images or sounds.

F. Employees will only utilize software provided and installed by ~~the Authority~~CFX's Information Technology Department. Additionally, you may not acquire, use, reproduce, transmit or distribute any controlled information including computer software and data, privacy information, copyrighted or trademarked material or material with other intellectual property rights or proprietary information without the IT Department's authorization.

G. All systems and equipment (workstations, laptops, desktops, servers, etc.) shall be secured and password protected when not attended.

H. For all systems under the control of the IT Department, the Administrator (admin) accounts cannot be disabled or altered in any way except by LAN Administrator /Help Desk personnel or the Information Security Manager. Any exception must be approved in writing by the IT Department.

I. All security breaches, suspected or otherwise, are to be immediately reported to the Information Technology Department.

J. All contractors who have access to sensitive and / or confidential information, including customer information, will be bonded by their employers and proof of such shall be available to ~~the Authority~~CFX upon request.

K. All employees will undergo a background check prior to employment and may be rechecked at any time during the employee's tenure.

L. All employees working in the CHDE (Card Holder Data Environment) are required to attend, on an annual basis, security awareness training.

III. Introduction to Facility Access Security Policy

The Central Florida Expressway Authority (CFX) recognizes the value of its employees and contractors in fulfilling its corporate mission. To that end, ~~the Expressway Authority~~CFX is committed to providing a safe and secure work environment. ~~The Central Florida Expressway Authority (CFX)~~CFX has established a facility access policy that shall be followed by all individuals working at or needing access to CFX Facilities. CFX Facilities are defined as all areas protected, either directly or indirectly, by CFX issued proximity cards. All permanent proximity badges are to be issued by the CFX IT Help Desk. All single day visitor badges are to be issued by the CFX ~~receptionist~~Front Office Administrator.

Proximity badges are in effect keys which grant physical access to both sensitive and / or non-sensitive areas of CFX Facilities. Proximity badges are to be treated with the same care as the username / password credentials utilized to access CFX computing resources. As such, proximity card PINs should never be written down or stored in any way. This includes writing the PIN in any form on the proximity card itself. For the purpose of this document, the following applies: "proximity card" and "badge" (when not referring to a visitor badge) are synonymous. Facility Employees shall be defined as all CFX personnel, contractors, consultants and vendors who require access to any CFX Facility.

IV. Facility Access Security Policy

A. Facility Employees

a. All Facility Employees will be issued a Facility Access badge per the Standard Operating Procedure IT-2 – Building Access and Account Request.

b. While on any CFX premises, the Facility Access badge shall be worn at all times on the Facility Employee's person where it is clearly visible.

c. Facility Employees will be given instructions pertaining to the proper use of the Facility Access badge at the time of employment.

d. The level of facility access will be approved by the CFX employee's manager or in the case of a non-CFX employee, the CFX Departmental Oversight Approver associated with the contractor, vendor and/or consultant.

e. All lost, stolen or defective Facility Access badges must be reported immediately by the respective Facility Employee to the following: Immediate supervisor, Departmental Oversight Approver for non-CFX employees and the CFX IT Help Desk.

f. Gaining entry into CFX Facilities either through tailgating and/or piggybacking is strictly prohibited. Tailgating and/or piggybacking is access gained by an authorized or non-authorized individual via the properly swiped Facility Access badge of an authorized Facility Employee. The only allowed exception is a properly signed in visitor(s) who is being escorted by a CFX Facility Employee.

g. The following is prohibited: sharing / lending of Facility Access badges; ownership of multiple active Facility Access badges; disclosure of PIN value.

h. No Facility Employee badge shall be issued without a photo ID being presented.

i. All managers must notify the IT Help Desk immediately upon termination of a badged individual.

j. All Facility Employees and Visitors must adhere at all times to the procedures and guidelines as set forth in the Standard Operating Procedure IT-2 – Building Access and Account Request and the Facility Security Procedure.

k. Any person requesting a Facility Access badge will be required to provide a valid driver's license, issued from the state of residence or a Florida Identification Card. This information will be stored inside the CFX's security system and will be utilized for identification purposes.

l. At the sole discretion of ~~the~~ CFX, this information may be shared with law enforcement. The driver's license information will not be otherwise released and is privileged from public records requests as provided for by Florida Statute.

m. Failure to adhere to the provisions of these documents could result in disciplinary action up to and including termination.

n. The procedures referenced in this policy are living documents and they will change from time to time in order to address needed changes.

V. HR~~,~~ and Director ~~and Deputy Director~~ Responsibilities

A. Ensure that all personnel under their supervision are aware of and comply with policies and procedures as related to the individual's job function.

B. The Director of Human Resources or his/her designee is responsible for providing a copy of this policy and the respective employee or contractor version of the 'Security Guidelines Handbook' and "Facility Procedures". Employees and contractors are to acknowledge in writing both receipt and understanding of the requirements of the respective document. The signed acknowledgement is to be placed in the employee's personnel file. Acknowledgement and receipt must occur on an annual basis for those individuals working in the CHDE environment.

C. Ensure proper disciplinary processes are followed when violations of this and other security procedures occur.

Central Florida Expressway Authority

Security Policy

Version 3.2

January 14, 2016

AMENDMENT REGISTER

Version No	Version Date	Amendment Description	Amended By
1.0	August, 2004	Original Version	Neal Jones, MSXI
1.1	November, 2005	Added Updates Required for PCI compliance	Bill Brownsberger, MSXI
2.0	October, 2006	Added Streaming Video and Audio Restrictions	Joann Chizlett
2.1	December, 2006	Added Instant Messaging Restriction	Bill Brownsberger, MSXI
2.2	May, 2008	Added file sharing and torrent sites Restrictions	Joann Chizlett
2.3	October, 2009	Rewrite and Reformat	Rene Rodrigue
3.0	November, 2009	Draft to Final	IT / Finance Dept
N/A	October 2013	Reviewed for PCI DSS Compliance	Rene Rodrigue
3.1	March 2014	Added Facility Access Policy Portion	IT / HR
3.2	January 2016	Modified for CFX	Corey Quinn

I. Introduction to Information Security Policy

Computer information systems and communications networks are integral and critical parts of the Central Florida Expressway Authority's (CFX) business operations. CFX has made a substantial investment to establish and protect these systems and the misuse of information or systems can do irreparable harm to the Authority, its employees and customers. It is therefore vital that all CFX staff and contractors commit to safeguarding these resources. Those who have access to CFX data are to use the utmost care in its protection from unauthorized disclosure, alteration, destruction or publication. Anyone responsible for the willful and negligent handling of CFX's systems, data or equipment shall be properly disciplined, up to and including termination and/or filing of a complaint with law enforcement.

CFX maintains many data files that are considered highly confidential from which negative consequences would ensue should the information be published or otherwise divulged negligently or maliciously. All confidential data must be treated as confidential with access limited to those whose access is required to perform their assigned duties. Staff is directed to implement security procedures that outline the care to be exercised by all employees and contractors related to CFX systems and equipment. In all cases where the correct course of action is uncertain, employees should always seek guidance from their supervisor or human resources representative. Contractors should seek guidance from their immediate supervisor and/or CFX contract point person.

CFX reserves the right, without notice or warning, at any time, to audit and / or monitor the use of CFX systems, data and / or equipment for the purpose of ensuring compliance with this and other security related documents such as the 'Employee Security Guidelines Handbook' and 'Contractor Security Guidelines Handbook'.

II. Information Security Policy

A. All computer system data and customer information that is maintained by CFX, whether electronic or hardcopy, is considered to be confidential unless specifically defined as open to the public.

B. All CFX employees and contractors are required to obtain written permission to disclose CFX information to anyone other than CFX employees or contractors who need the information to conduct their official business. All other requests for information, except for inquiries from the media, shall be routed through CFX's Records Custodian who will determine if information is legally public record prior to its release. If there is any doubt as to the information's legal status, General Counsel shall be consulted. Requests for information from the media shall be routed through the Marketing and Communications Department.

C. All employees and contractors must adhere at all times to the processes, procedures and guidelines as set forth in their respective 'Security Guidelines Handbook', i.e. the 'Employee Security Guidelines Handbook' or the 'Contractor Security Guidelines Handbook'. Failure to adhere with the provisions of these respective documents, as applicable to employee or contractor, could result in disciplinary action up to and including termination. Additionally, civil penalties and fines could also apply. The above documents are living documents and they will change from time to time in order to add, delete or modify processes, procedures and / or guidelines.

D. Employees and contractors will only use CFX systems, information and equipment in a manner consistent with the employees and / or contractor's job function and requirements. CFX resources are to be used for CFX business only.

E. You may not access or disseminate material that is offensive, harassing or illegal (ex. software piracy) in nature, including but not limited to material that disparages others based on race, religion, ethnicity, gender, sexual orientation, age, disability or political affiliation. In addition, you may not access or disseminate sexually explicit or sexually oriented messages, images or sounds.

F. Employees will only utilize software provided and installed by CFX's Information Technology Department. Additionally, you may not acquire, use, reproduce, transmit or distribute any controlled information

including computer software and data, privacy information, copyrighted or trademarked material or material with other intellectual property rights or proprietary information without the IT Department's authorization.

G. All systems and equipment (workstations, laptops, desktops, servers, etc.) shall be secured and password protected when not attended.

H. For all systems under the control of the IT Department, the Administrator (admin) accounts cannot be disabled or altered in any way except by LAN Administrator /Help Desk personnel or the Information Security Manager. Any exception must be approved in writing by the IT Department.

I. All security breaches, suspected or otherwise, are to be immediately reported to the Information Technology Department.

J. All contractors who have access to sensitive and / or confidential information, including customer information, will be bonded by their employers and proof of such shall be available to CFX upon request.

K. All employees will undergo a background check prior to employment and may be rechecked at any time during the employee's tenure.

L. All employees working in the CHDE (Card Holder Data Environment) are required to attend, on an annual basis, security awareness training.

III. Introduction to Facility Access Security Policy

The Central Florida Expressway Authority (CFX) recognizes the value of its employees and contractors in fulfilling its corporate mission. To that end, CFX is committed to providing a safe and secure work environment. CFX has established a facility access policy that shall be followed by all individuals working at or needing access to CFX Facilities. CFX Facilities are defined as all areas protected, either directly or indirectly, by CFX issued proximity cards. All permanent proximity badges are to be issued by the CFX IT Help Desk. All single day visitor badges are to be issued by the CFX Front Office Administrator.

Proximity badges are in effect keys which grant physical access to both sensitive and / or non-sensitive areas of CFX Facilities. Proximity badges are to be treated with the same care as the username / password credentials utilized to access CFX computing resources. As such, proximity card PINs should never be written down or stored in any way. This includes writing the PIN in any form on the proximity card itself. For the purpose of this document, the following applies: "proximity card" and "badge" (when not referring to a visitor badge) are synonymous. Facility Employees shall be defined as all CFX personnel, contractors, consultants and vendors who require access to any CFX Facility.

IV. Facility Access Security Policy

A. Facility Employees

a. All Facility Employees will be issued a Facility Access badge per the Standard Operating Procedure IT-2 – Building Access and Account Request.

b. While on any CFX premises, the Facility Access badge shall be worn at all times on the Facility Employee's person where it is clearly visible.

c. Facility Employees will be given instructions pertaining to the proper use of the Facility Access badge at the time of employment.

d. The level of facility access will be approved by the CFX employee's manager or in the case of a non-CFX employee, the CFX Departmental Oversight Approver associated with the contractor, vendor and/or consultant.

e. All lost, stolen or defective Facility Access badges must be reported immediately by the respective Facility Employee to the following: Immediate supervisor, Departmental Oversight Approver for non-CFX employees and the CFX IT Help Desk.

f. Gaining entry into CFX Facilities either through tailgating and/or piggybacking is strictly prohibited. Tailgating and/or piggybacking is access gained by an authorized or non-authorized individual via the properly swiped Facility Access badge of an authorized Facility Employee. The only allowed exception is a properly signed in visitor(s) who is being escorted by a CFX Facility Employee.

g. The following is prohibited: sharing / lending of Facility Access badges; ownership of multiple active Facility Access badges; disclosure of PIN value.

h. No Facility Employee badge shall be issued without a photo ID being presented.

i. All managers must notify the IT Help Desk immediately upon termination of a badged individual.

j. All Facility Employees and Visitors must adhere at all times to the procedures and guidelines as set forth in the Standard Operating Procedure IT-2 – Building Access and Account Request and the Facility Security Procedure.

k. Any person requesting a Facility Access badge will be required to provide a valid driver's license, issued from the state of residence or a Florida Identification Card. This information will be stored inside the CFX's security system and will be utilized for identification purposes.

l. At the sole discretion of CFX, this information may be shared with law enforcement. The driver's license information will not be otherwise released and is privileged from public records requests as provided for by Florida Statute.

m. Failure to adhere to the provisions of these documents could result in disciplinary action up to and including termination.

n. The procedures referenced in this policy are living documents and they will change from time to time in order to address needed changes.

V. HR and Director Responsibilities

A. Ensure that all personnel under their supervision are aware of and comply with policies and procedures as related to the individual's job function.

B. The Director of Human Resources or his/her designee is responsible for providing a copy of this policy and the respective employee or contractor version of the 'Security Guidelines Handbook' and "Facility Procedures". Employees and contractors are to acknowledge in writing both receipt and understanding of the requirements of the respective document. The signed acknowledgement is to be placed in the employee's personnel file. Acknowledgement and receipt must occur on an annual basis for those individuals working in the CHDE environment.

C. Ensure proper disciplinary processes are followed when violations of this and other security procedures occur.