

Bernard Smith, Chairman
Stephen Auger, Executive Director

Brian Katz, Audit Committee Chairman
Chris Hirst, Inspector General

Final Report
Project #2014-07 Audit of Information Technology Policies July 1, 2014

SUMMARY

The Office of Inspector General conducts audits of Florida Housing Finance Corporation's (Corporation) programs to provide management and other stakeholders with unbiased, timely, and relevant information for use in promoting accountability, stewardship and efficient operations.

Our audit disclosed that information technology policies had been developed addressing most of the areas identified in best practice guidance; however, some key areas did not have adequate coverage.

OBJECTIVES, SCOPE AND METHODOLOGY

At the request of the Chief Technology Officer (CTO) during our annual risk assessment and in accordance with the Office of Inspector General's (OIG) Annual Audit Plan for Fiscal Year 2014, we conducted this audit. Our audit objective was to determine the adequacy of the information technology (IT) policies of the Corporation.

The audit covered the IT policies which were in effect at the time of our review.¹ Those policies were as follows:

- 7100 General Acceptable Use
- 7120 Email Acceptable Use
- 7130 Remote Access
- 7140 Virtual Private Network
- 7150 Wireless Network
- 7160 Personal Mobile Device Policy
- 7170 Information Security Program

To achieve our audit objective, we performed the following:

- Reviewed the results of the OIG's June 2013 management review of IT policies;
- Researched laws, rules and regulations to identify those governing the Corporation's IT function;
- Reviewed industry best practices identified in literature² from IT-related organizations, such as:
 - Control Objectives for Information and Related Technology (COBIT 5);

¹ This audit did not address implementation of the policies or staff's compliance with the policies. Those areas may be included in future audit plans as determined by the results of annual risk assessments.

² See Appendix A for descriptions of the sources of best practices guidance used for this audit.

- Chapter 71A-1, Florida Administrative Code, *Florida Information Technology Resource Security Policies and Standards*;
- Global Information Assurance Certification (GIAC);
- The National Institute of Standards and Technology (NIST);
- The SANS Institute; and
- UNINETT (Norwegian Network for Research and Education);
- Developed Attribute Checklists based on industry best practices to identify the attributes that should be present in each policy;
- Interviewed appropriate management and staff;
- Reviewed appropriate Corporation documentation; and
- Compared the Corporation's IT policies to industry best practices.

BACKGROUND

A policy is a “formal, brief, high-level statement or plan that embraces an organization’s general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policy attributes include the following:³

- Require compliance (mandatory)
- Failure to comply results in disciplinary action
- Focus on desired results, not on means of implementation
- Further defined by standards and guidelines”

According to the SANS Institute, it is the responsibility of the IT managers and staff to develop and oversee the implementation of the IT policies. Written policies ensure that executive management’s expectations are documented, roles and responsibilities are defined and staff have guidance for maintaining information security.

The current IT policies, as listed in the section above, were developed by the staff of the Corporation’s Information Technology Section (ITS) and, in 2013, were approved by the Executive Director. The policies are posted on the Corporation’s intranet site and are part of the *Employee Policy and Procedures Handbook*.

FINDINGS AND RECOMMENDATIONS

Information technology frameworks (such as NIST and COBIT 5) and state agency regulations (such as Chapter 71A-1, Florida Administrative Code) identify accepted industry best practices for developing a robust IT policy. Suggested components and structure are detailed in various documents, position papers, primers and training materials as identified in Appendix A. Our comparison of the Corporation’s IT policies to accepted best practices disclosed that the policies addressed most of the key components identified in best practices, but some areas did not have adequate coverage. Those areas needing improvement are discussed below.

³ Source: The SANS Institute - *A Short Primer of Developing Security Policies*

Finding 1 – Incident Response Plan

Best practices for IT policies suggest establishing a security incident response plan for identifying and controlling the suspected computer security incidents, notifying designated responders and reporting outcomes to executive management. The Corporation's incident response plan, currently included in Policy #7170 - *Information Security Program*, addresses incidents where "personally identifiable information is subject to suspected and/or accidental public release or unauthorized access is extremely serious ..." However, the following key components as recommended in best practices were not addressed:

- Having a stand-alone incident response policy. The current placement of the incident response requirements within the Information Security Program policy makes the requirements difficult to find when guidance is needed for responding to an incident. A stand-alone policy, with its own policy number assigned, would be easier to locate in the list of IT policies.
- Treating all breaches of security, along with the improper use of information systems, as incidents. Since the current policy only addresses incidents related to personally identifiable information, staff are not provided guidance on other types of breaches that should be reported and how they should be handled
- Defining various levels of incidents and, generally, how to handle each. For example, low-level incidents might be managed automatically by the security infrastructure with minimal response from a human administrator. Mid-level incidents may require an internal investigation by the Office of Inspector General. High-level incidents may require the involvement of law enforcement. Without categories, the same level of response and reporting is applied to all incidents resulting in staff resources not being allocated in the most efficient manner.

We recommend that the Corporation develop a stand-alone incident response policy encompassing these key components to ensure that Corporation staff can readily locate the policy. The policy should inform staff of their responsibilities for responding to any computer security incident, not just those related to PII.

Finding 2: Data Classification Policy

Best practices recommend that information security policies include a data classification policy. Such a policy should state the Corporation's general beliefs, goals and plans with regard to its data classification system. A data classification system provides a mechanism for sorting and labeling every type of data, identifying its value, importance, sensitivity, cost, and other concerns in order to guide the implementation of security and prescribe processes for management and use. Assigning classification labels, such as public, private, sensitive, internal only, confidential, proprietary, etc., helps staff understand how to use and handle resources properly. Those resources with moderate to high value and sensitivity require greater control and tighter security. Such a system would provide assurance that the confidentiality, integrity and availability of the Corporation's data is properly maintained.

The Corporation does not have a data classification policy documenting the Corporation's position, goals and objectives for information classification. Without a policy, data may not be properly classified; data owners may not adequately understand what their responsibilities are; they may not adequately communicate data security requirements to staff charged with developing, deploying, maintaining and

monitoring the systems that contain the data; and staff may not use appropriate controls when working with data.

We recommend that the Corporation develop and implement a data classification policy to ensure the confidentiality, integrity and availability of the Corporation's data is properly maintained.

Finding 3: Training

Information technology best practices recommend that an organization perform due-diligence in educating users on the security requirements of their jobs, including the information security policies and procedures that apply to them. Some guidance requires that workers receive initial security awareness training within 30 days of employment start date and “initial training shall include acceptable use restrictions, procedures for handling exempt, and confidential and exempt information, and computer security incident reporting procedures.”⁴

The Corporation's *Information Security Program* policy states employees should receive training on the security, confidentiality and integrity of Personally Identifiable Information (PII). The policy also states that “all employees have been instructed regarding Florida Housing's Policy – and the legal requirement to keep Personally Identifiable Information secure and confidential.” However, we noted that the policy does not require that:

- new employees receive training on all IT security policies and
- current employees receive training when there are significant changes in IT policies due to events such as new laws, new compliance requirements, new technology rollouts or changes in management's philosophy regarding IT resources and security.

Not requiring training of new staff or notifying current staff of policy changes in a timely manner could put the Corporation's IT systems at risk because new staff may not be aware of their responsibilities regarding security. Also, without having received training current staff may not be aware of their revised responsibilities in the event of policy changes.

We recommend that the IT policies be revised to require training of all new employees on all areas of IT security and training of all current employees on significant policy changes. The policies should include a specified timeframe after hiring and after the policy change for the training to occur.

Finding 4: Identification of Disciplinary Actions for Policy Violations

Most IT security best practices recommend that IT policies contain language addressing how the policy will be enforced and how violations will be handled.

The Corporation's IT policies do not contain language informing the reader how the policies will be enforced or the ramifications for violations of policy. This information was only found in the *Employee Acknowledgment and Disclosure Agreement* which new staff sign on their first day of employment. The Agreement states the following in the General Terms section:

⁴ Rule 71A-1.008(5), Florida Administrative Code

I understand and agree that failure to comply with the terms of this Agreement could result in disciplinary action, including termination of employment. I agree that should the Corporation deem it necessary to take legal action to rectify the effects of my violation or prevent further harm to the Corporation that I will be responsible for all attorney's fees and court costs incurred by the Corporation.

While the Agreement notifies staff of the Corporation's general disciplinary policy, employees may not remember it since it is only brought to their attention on their first day of employment. Without the disciplinary policy being specifically addressed in the IT policies, staff may not understand how serious the Corporation considers violations of IT policies to be and the possible consequences for violating the policies.

We recommend that the Corporation include language in the IT policies addressing how those policies will be enforced and how violations will be handled.

OTHER - ATTRIBUTE CHECKLISTS FOR IT POLICIES

Based on a combination of industry best practices, the audit staff developed an Attribute Checklist for evaluating each of the Corporation's IT policies. The completed checklists were provided to the CTO for use in revising the IT policies and ensuring that key components are addressed. To facilitate the revision process, we also provided the CTO with a copy of each policy documenting the auditor's comments and suggested changes.

RESPONSE

In a response letter dated June 30, 2014, management concurred with our recommendations. The response is included in this report as Attachment B.

ACKNOWLEDGEMENT

The Office of Inspector General would like to extend our appreciation to the management and staff of the Corporation for their assistance and cooperation during this audit.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors. The audit was conducted by David Merck, CISA, CISSP, CAP, under the supervision of Kim Mills, Director of Auditing, CPA, CGFM, CIG. This report and other reports prepared by the Office of the Inspector General can be obtained from the Corporation's website, <http://www.floridahousing.org/AboutUs/OfficeOfInspectorGeneral>.

APPENDIX A –SOURCES OF BEST PRACTICES GUIDANCE

COBIT 5, A Business Framework for the Governance and Management of Enterprise IT

COBIT 5 - Control Objectives for Information and Related Technology: enables clear policy development and good practices for IT control throughout organizations. COBIT 5 emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the enterprise's IT governance and control framework.

GIAC, How to Develop Good Security Policies and Tips on Assessment and Enforcement

GIAC - Global Information Assurance Certification: an information security certification entity and leading publisher of information security guidelines and best practices.

NIST Special Publications 800-12, 800-53 and 800-100

NIST - National Institute of Standards and Technology: an agency in the Technology Administration of the U. S. Department of Commerce that NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002 (FISMA) and to help with managing cost effective programs to protect their information and information systems.

- *Publication 800-12: An Introduction to Computer Security: The NIST Handbook – Computer Security.* This handbook illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.
- *Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.* This publication provides a catalog of security controls for all U.S. federal information systems except those related to national security.
- *Publication 800-100: Information Security Handbook - A Guide for Managers, Information Security.* This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.

Chapter 71A-1, Florida Administrative Code, Florida Information Technology Resource Security Standards

Chapter 71A-1, Florida Administrative Code, provides a framework of information security best practices for state agencies in order to safeguard the confidentiality, integrity, and availability of Florida government data and information technology resources.

The SANS Institute, A Short Primer for Developing Security Policies

The SANS Institute is a cooperative research and education organization. Their programs now reach more than 165,000 security professionals around the world including auditors and network administrators, to chief information security officers in varied global organizations from corporations to universities. SANS also develops, maintains, and makes available at no cost, a large collection of research documents about various aspects of information security.

UNINETT, Information Security Policy Best Practice Document

UNINETT develops and operates the Norwegian national research and education network, a high-capacity computer network interconnecting about 200 Norwegian educational and research institutions and more than 300,000 users. The company supplies a range of services connected with the research network, among other things in the fields of identity management, purchasing co-operation, mobility, network management and security.

APPENDIX B – MANAGEMENT'S RESPONSE

(Continued on next page)

July 1, 2014

Mr. Chris Hirst, Inspector General
Florida Housing Finance Corporation
227 N Bronough Street, Suite 5000
Tallahassee, FL 32301

RE: Preliminary Findings and Recommendations from the Audit of Information Technology Policies

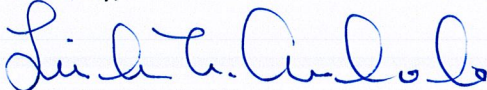
Dear Mr. Hirst:

In accordance with Section 20.055, Florida Statutes, enclosed you will find our response to the Preliminary Findings and Recommendations from the Audit of Information Technology Policies dated June 11, 2014.

We appreciate the time and energy put forth by your staff during this process. The recommendations certainly add value as we move forward with updating the Information Technology policies. I look forward to working with you and your team in the future.

If you have questions or need additional information regarding this response, please contact me at (850) 488-4197.

Sincerely,



Linda M. Arredondo
Chief Technology Officer

Enclosure

Cc: Bernard Smith, Chairman
Stephen P. Auger, Executive Director
Brian Katz, Chairman, Audit Committee

Rick Scott, Governor

Board of Directors: Bernard "Barney" Smith, Chairman • Natacha Munilla, Vice Chairman
Ray Dubuque • John David Hawthorne Jr. • Brian Katz • Leonard Tylka • Howard Wheeler
Bill Killingsworth, Florida Department of Economic Opportunity

Executive Director: Stephen P. Auger

Response to the Preliminary Findings and Recommendations
from the
Audit of Information Technology Policies

Finding 1: We recommend that the Corporation develop a stand-alone incident response policy encompassing these key components to ensure that Corporation staff can readily locate the policy. The policy should inform staff of their responsibilities for responding to any computer security incident, not just those related to Personally Identifiable Information (PII).

Response 1 - Information Technology Services (ITS) shall:

1. Develop a draft incident response policy by August 1, 2014.
2. Engage in a collaborative review which may include ITS, Office of Inspector General (OIG), Legal, Human Resources (HR) and/or other business units as appropriate.
3. Obtain the necessary quotes to submit with the 2015 Budget Request if implementation of the policy requires ITS staff training and /or new hardware and software.
4. Finalize the incident response policy (pending budget approval) and submit for signature by April 1, 2015.
5. Embark on the Implementation Phase by introducing the new policy via the ITS Training Framework by July 1, 2015.

Finding 2: We recommend that the Corporation develop and implement a data classification policy to ensure the confidentiality, integrity and availability of the Corporation's data is properly maintained.

Response 2 - ITS shall:

1. Develop a draft data classification policy by August 1, 2014.
2. Engage in a collaborative review which may include ITS, OIG, Legal, HR and/or other business units as appropriate.
3. Obtain the necessary quotes to submit with 2015 Budget Request if implementation of the policy requires ITS staff training and /or hardware and software.
4. Finalize data classification policy (pending budget approval) and submit for signature by the April 1, 2015.
5. Embark on the Implementation Phase by introducing the new policy via the ITS Training Framework by July 1, 2015.

Finding 3: We recommend that the Information Technology policies be revised to require training of all new employees on all areas of IT security and training of all current employees on significant policy changes. The policies should include a specified timeframe after hiring and after the policy change for the training to occur.

Response 3 - ITS shall:

1. Revise the ITS Policy "7100 General Acceptable Use" to include a section titled "ITS Training Framework" by August 1, 2014. Specifications for the ITS Training Framework will include:
 - a. Annual Security Awareness Training;
 - b. Annual ITS Policy Training;
 - c. Definition of significant policy changes;
 - d. Parameters for rolling out significant policy changes; and
 - e. ITS Security Awareness and Policy Training for new hires within 30-days of employment.
2. Initiate implementation of the ITS Training Framework by September 1, 2014.

Response to the Preliminary Findings and Recommendations
from the
Audit of Information Technology Policies

Finding 4: We recommend that the Corporation include language in the IT policies addressing how those policies will be enforced and how violations will be handled.

Response 4 - ITS agrees that it is important for all employees to acknowledge their understanding of how policy violations will be enforced and handled. ITS will:

1. Initiate a collaborative review of the current *Employee Acknowledgment and Disclosure Agreement* which may result in enhancing and/or clarifying the content of the form. The collaborative review may include ITS, OIG, Legal, HR and/or other business units as appropriate.
2. As part of the collaborative review, consider asking or requiring each employee to sign the *Employee Acknowledgment and Disclosure Agreement* upon completion of each ITS Training opportunity, as provided by the ITS Training Framework.
3. Develop training slides to highlight how violations of the ITS policies will be enforced and handled.
4. Initiate implementation of the new training slides via the ITS Training Framework by September 1, 2014.