DIFS DEPARTMENT OF INSURANCE AND FINANCIAL SERVICES *Office of Credit Unions* *Policies and Procedures*	POLICY NUMBER 10605 EFFECTIVE DATE 11/01/2018
EXAMINATION	REVISION DATE 11/28/2023
SUBJECT	PAGE(S)
Information Technology and Security	**Page 1 of 3**

I. PURPOSE

Examiners must assess information technology complexity and management's oversight of information security. The Gramm-Leach-Bliley Act (GLBA) provides a minimum compliance governance framework. Examiners should evaluate industry accepted security standard practices and guidelines and their integration with the institution's operations and environment. Without appropriate information security controls and oversight, management places consumers' personally identifiable information at risk, which in return, places the institution's reputation at risk. Since information technology is integrated throughout operations, numerous inherent risks exist which impact institutions.

II. PRIMARY REFERENCES / RELATED REGULATIONS

1. Office of Credit Union:
   a. *2003 PA215 - Michigan Credit Union Act:*
      - Section 490.408 – Automated Information Processing Services
      - Section 490.407 – Credit Union Service Organizations

   b. *OCU Letters and Bulletins:*
      - Letter 2007-CU-03: 2006 Identity Theft Protection Act and Incident Response Plans.
      - Letter 2006-CU-07: Information Technology (IT) Examinations
      - Letter 2005-CU-10: Contingency Planning
      - Letter 2005-CU-09: Internet Financial Services
      - Letter 2005-CU-01: Gramm-Leach-Bliley Act of 1999 (GLBA)
      - Bulletin No. 2005-06-CU: Information Security Program
2. Federal:
      - 12 CFP 1016 – CFPB: Privacy of Consumer Financial Information
      - Part 740 – NCUA Rules and Regulation: Accuracy of Advertising
      - Part 748 – NCUA Rules and Regulations: Security Program (GLBA enforcement)

   b. *Guidance Letters:*
      - Refer to NCUA's or FFIEC's website for detailed letters.

3. General Industry References
   a. *Website References:*
      - FFIEC IT Examination Handbook InfoBase - Home
      - www.isaca.org/

- www.nist.gov/ (information technology and cybersecurity)
- www.fdic.gov/resources/supervision-and-examinations/
- www.occ.treas.gov/
- www.ncua.gov
- www.sans.org/

III. BACKGROUND

Protection of information assets is essential in establishing and maintaining trust between an institution and consumers. Information technology involves physical and logical security surrounding the network and core data applications. Furthermore, information technology involves system development lifecycle concerns and technology (hardware/software) replacement processes. It includes disaster recovery and business continuity concerns. Information systems also include electronic banking services delivery, website governance, and social media usage. With the advent of new technologies, it also includes cloud computing and the Internet-of-Things (IoT). As a result of the width and depth of this area, management teams are expected to use and to document an IT risk-based audit.

Information security is governed by the Gramm-Leach-Bliley Act (GLBA), as enforced by 12 CFR, NCUA's Rules and Regulations, Part 748. The focus of GLBA involves:

- Information security risk assessment.
- Information security program.
- Vendor management oversight
- Testing of key information security controls.
- Employee information security awareness training.
- Privacy information concerns.
- GLBA compliance status report to the Board.

IV. MINIMUM PROCEDURES

Examiners are responsible for reviewing all operational aspects of an institution, including information technology and information security. Examiners will complete the IT Follow-Up Work-Program during each examination unless a full IT examination was performed within the prior 12 months or is being performed concurrently. Supervisors must ensure a full IT examination, including the issuance of full URSIT ratings, is performed no less than once every 36 months. Examiners will review the prior IT examination and assess the status of corrective action. Examiners who identify significant deficiencies when completing the IT Work-Programs or performing IT examination follow-up should notify their supervisor so appropriate IT examination resources can be allocated.

The Office of Credit Unions (OCU) has the authority to examine third-party service providers. This review is to the same extent that OCU examines a credit union. Examinations are scheduled as appropriate. These examinations will use the FFIEC's IT work programs, the InTREx work programs, or another designated OCU IT program.

V. ATTACHMENTS / FORMS

- URSIT Work-Program
- IT Follow-Up Work-Program
- InTREX-CU Workbook
- FFIEC's Work programs – refer to work programs updated on ithandbook.ffiec.gov.