**While the FFIEC does not have information regarding insider threats directly there is guidance on several subjects directly relating to the subject, which we have provided below.**

**Sources Concerning: Insider Threats As of 3/2/20.**

**DISCLAIMER:** *While we attempt to assert that this document includes all information available on the ffiec.gov website as of the date listed above, we offer this as an aid to audit and consulting Clients, and in no way warrant this as being all-inclusive, complete, or thorough. Please use at your own risk.*

Resources:  
**FFIEC IT Examination Handbook**Information Security Booklet  
II.C.7: User Security Controls  
*https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls.aspx* (Accessed 3/2/20)

Users should be granted access to systems, applications, and databases based on their job responsibilities. Access rights should be granted in accordance with the institution's physical and logical access control policies. Authorized users with elevated or administrator privileges can pose a potential threat to systems and data. Employees, contractors, or third-party service providers can exploit their legitimate computer access for unauthorized purposes. Additionally, the degree of internal access granted to some users increases the risk of damage or loss of information and systems. Risk exposures from internal users include the following:

* Alteration of data.
* Deletion of production and backup data.
* Misdirected data.
* Disruption of systems.
* Destruction of systems.
* Misuse of systems for personal gain or to damage the institution.
* Appropriation of strategic or customer data for espionage or fraud schemes.
* Extortion for stolen data.
* Misuse of data following the termination or change in job responsibility of an employee.

Management should understand the risks to the institution's information-processing environment and establish appropriate user access controls to mitigate these and other potential risks to the institution's assets. Users should understand and confirm their understanding of their roles and responsibilities in maintaining a sound security environment, which includes both physical and logical areas.

**FFIEC IT Examination Handbook**Information Security Booklet  
II.C.7(a): Security Screening in Hiring Practices  
*https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(a)-security-screening-in-hiring-practices.aspx* (Accessed 3/2/20)

Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system misuse or fraud.

**FFIEC IT Examination Handbook**Information Security Booklet  
II.C.7(b): User Access Program  
*https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(b)-user-access-program.aspx* (Accessed 3/2/20)

Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements:

* Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity.
* Alignment of employee job descriptions to the user access program.
* Requirements for business and application owners to define user profiles.
* Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel.
* Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations.

Periodic independent reviews that ensure effective administration of user access, both physical and logical.

For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.

**FFIEC IT Examination Handbook**Information Security Booklet  
II.C.7(c): Segregation of Duties  
*https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(c)-segregation-of-duties.aspx* (Accessed 3/2/20)

Segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk. Employees and third parties with access to sensitive resources could cause substantial damage and potential loss. System administrators, for instance, have the most powerful role in the user access process and have unlimited access to an institution's information assets and technology. Given this extensive access, management should evaluate the process for determining which individuals should be granted system administrator privileges. Such access should be appropriately monitored for unauthorized or inappropriate activity. Management should incorporate independent reviews or approvals for individuals who perform multiple functions to minimize the potential for fraud, irregularities, and errors. Examples of segregation of duties include the following:

* Independent monitoring of the activities performed by the users with increased privileges (e.g., system administrators and super users).
* Distribution of system administration activities so no administrator can hide his or her activities or control an entire system.
* Additional levels of approval as the criticality and sensitivity of decisions increase.

If an activity is conducted without appropriate segregation of duties, management should require an independent review (e.g., audit) of that activity.

**FFIEC IT Examination Handbook**Information Security Booklet  
II.C.7(d): Confidentiality Agreements  
*https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(d)-confidentiality-agreements.aspx* (Accessed 3/2/20)

**II.C.7(d)     Confidentiality Agreements**

The institution should protect the confidentiality of customer and institution information. A breach in confidentiality could disclose proprietary information, increase fraud risk, damage the institution's reputation, violate customer privacy and associated rights, and violate laws or regulations. Confidentiality agreements can be used to put all parties on notice that the financial institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs. Management should obtain signed confidentiality agreements before granting employees and contractors access to IT systems.

**FFIEC IT Examination Handbook**Information Security Booklet  
II.C.7(e): Training  
*https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic7-user-security-controls/iic7(e)-training.aspx* (Accessed 3/2/20)

Training ensures personnel have the necessary knowledge and skills to perform their job functions. Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance.

Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program.