Policy and Procedures Statement

Policy Title: **DAC-FICRAS Service System Policy and Procedures Statement**

Re: **DAC-FICRAS SA – 18001**

Brief Description:	This Policy and Procedures Statement will address the various DAC-FICRAS Service System operational and administrative rules that will be used in guiding authorized DAC-FICRAS and client personnel in their activities while working within the DAC-FICRAS Service System environment.
Effective:	July 12, 2018
Approved on Behalf of:	DAC Governance Committee
Approved by:	DAC Governance Executive Committee Chair, Lawrence J. Golicz, PhD., MAI, ASA
DAC Responsible Officer (RO): RO Contact Information:	DAC-FICRAS Services Administrator, Gregory G. Johnson, MAI, SR/WA Email: administration@ficras.com Phone: 727-919-1611
Supersedes:	All prior policies, verbal or written
Last Reviewed/Updated:	April 1, 2024
Applies to:	This document is applicable to all DAC-FICRAS authorized personnel, including officers, associates, employees, contractors, and contractor employed personnel who provide service to DAC-FICRAS operations. Each is required to be aware of and correctly employ the policy and procedures established herein. If any authorized user ("constituent") is confused regarding a policy or procedure, they are instructed to contact the DAC Responsible Officer identified above. Also, clients, their valuation service providers, other ancillary service providers, their contractors and contractor employed personnel who may be authorized as users, providers and/or contributors of the DAC-FICRAS Service System, each, individually acknowledge and agree to comply with this Policy and Procedures Statement, recognizing this is required to continue their system use authorization. Any constituent's authorization may be summarily and immediately halted for non-compliance.

Reason for Policy and Procedure Statement – The purpose of this statement is *documentation* of operational and administrative rules to guide authorized DAC-FICRAS Service System personnel, authorized clients and their personnel in their day to day activities as they interface with the DAC-FICRAS Service System.

INTRODUCTION:

It is the intent of this Policy and Procedure Statement to outline and describe all operational and administrative policy and procedures that would potentially affect the continued development, maintenance and operation of any component of the DAC-FICRAS Service System. If any reader should identify issues that they believe should be covered, that are not covered here, please direct an inquiry to the Responsible DAC Officer identified above. Although every effort has been made to cover policy and procedures for all operational and administrative DAC-FICRAS Service System components, it is not uncommon that some can be missed. We are ready and prepared to review any inquiry and modify this Policy and Procedure Statement if it is determined to be required. Thank You.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

POLICY STATEMENT:

It is the policy of the DAC-FICRAS Service System to ensure its integrity by implementing various policy and procedures to enable authorized users of the system to recognize and understand the active processes to be followed in the event of operational or administrative issues that could affect the lawful use of the DAC-FICRAS Service System. Policy extends to all operational and administrative functions of the DAC-FICRAS Service System. It is the duty of each authorized user and contributor to be aware of and adhere to the policy and procedures contained herein. Any authorized user who does not comply with the policy and procedures recited herein, could have their DAC-FICRAS Service System user or contributor authorization revoked at any time for non-compliance.

DEFINITIONS:

Anyone having questions regarding definitions is directed to notify the Responsible DAC Officer referred to on page 1 of this document. Definitions and references are made within the text of each policy and procedures component as they are written and generally are identified as (definition) within the text.

HISTORY:

The DAC-FICRAS Service System has been in operation since November 2014. It serves the valuation service needs of its financial institution clients through a secure web-based environment that is professionally managed both operationally and administratively. Heretofore, the operations and administrative management was closely held among a small number of specialists who collaborated and communicated daily. With the growth of the DAC-FICRAS system, some of the closely held information requires distribution to a growing list of associates. Additionally, the operational and administrative needs of clients and the internal DAC-FICRAS administration has required that formal policy and procedures requirements are communicated and distributed to all authorized users and contributors and that each recognizes the importance of following the policy and procedures in serving DAC-FICRAS clients or in serving the DAC-FICRAS service system itself.

POLICY AND PROCEDURES:

Code of Conduct Policy and Procedures:

Code of Conduct Policy Statement:

DAC-FICRAS operations deal principally with providing valuation service capabilities to its clients. In this regard, part of this Code of Conduct policy requires all personnel, whether employees, contractors, contributors, or other providers who either represent the company or participate in providing services to it and/or its clients, to be aware of and adhere to the provisions of the Uniform Standards of Professional Appraisal Practice (USPAP) as promulgated from time to time by the Appraisal Foundation. Also, this policy requires of the same constituents referred to above, to be aware of and adhere to the Code of Professional Ethics and Standards of Professional Practice as may be promulgated from time to time by the Appraisal Institute, when mandated by law, regulation or agreement.

In all DAC-FICRAS Service System business activities, all personnel shall adhere to all Federal, state and local laws pertaining to legal requirements that may affect their services on behalf of the DAC-FICRAS Service System. This includes any and all anti-discrimination, privacy, employment, tax, disclosure, confidentiality, and all other laws and regulations that affect operation of the DAC-FICRAS Service System. It is the intent of this Code of Conduct to ensure intra and inter-company relationships are based on respect for all constituents, with each providing caring, timely response to any questions or communications received by or distributed from any member of the DAC-FICRAS Service System team. The guiding principle in all DAC-FICRAS Service System activities is the "Golden Rule"; "to do for others as you would wish them to do for you".

Code of Conduct Procedures:

If any question should arise regarding this Code of Conduct Policy, they shall be addressed to the following DAC-FICRAS responsible officer for investigation and response:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

Security Policy and Procedures:

Security Policy Statement:

It is the DAC-FICRAS Service System policy to provide the highest level secure environment in hosting client, provider and contributor applications and data. This is accomplished through system, application, communications, and personal security measures established to conduct the necessary operations and administrative functions required by the DAC-FICRAS Service System and the various client, provider and contributor authorized users we serve.

System Security – FICRAS servers are designed as an array spread across multiple backbones with our primary secure network operations located in Tampa, Florida, within the WOW! Enterprises, LLC network operations center (NOC) [about-WOW]. All data are backed up by redundant servers in other locations and are monitored and managed 24/7/365 by not only WOW! personnel, but also by FICRAS's data networking provider, Webtent Networking, Inc., http://www.webtent.net/, who serves as webmaster and system security agent for FICRAS Webtent provides a redundant private server array, in multiple (NOC) locations and is positioned to provide real time system management and maintenance to ensure data integrity and continued service. At a minimum, all systems are backed up daily, with data servers being mirrored and backed up hourly to ensure minimal loss in the event of system outage. Additionally, back up cycles can be provided directly to clients wishing to host their own data. Each server has the latest software and firewall packages and is constantly monitored for potential security vulnerabilities and intrusion attempts.

[Note: A copy of the most recent WOW! Enterprises SOC 1, Type 2 Report, will be provided to any authorized DAC-FICRAS Service System user upon request to the DAC Responsible Officer identified in page 1 of this report].

Application Security – Information passed to FICRAS application processors, whether from the URL string, via POST or passed directly to the control port is rigorously checked for the latest security vulnerabilities. Only specific sequences, properly identified, are processed. Our applications know what to expect and will only accept information appropriate to the functions being used. All SQL is verified prior to execution. For each, an expected result is calculated and matched against the final result before committing changes to any database. It is the intent of this policy

Security Policy and Procedures: (Continued)

Security Policy Statement: (Continued)

to provide the most rigorous assessment of application services. All application processes are monitored in real time by system administrator to ensure application and data integrity.

Communication Security – All communication between the user and host are encrypted. FICRAS supports all non-vulnerable SSL and TLS encryption protocols (up to 2048-bit). FICRAS adheres to the latest encryption standards and encryption is provided across the FICRAS network to serve all web device protocols. To independently access the QUALYS SSL Labs server test system for the FICRAS website, please follow this link [QUALYS SSL Test] and enter the website name www.ficras.com.

Personal Security – FICRAS does not gather, store or disseminate any private personal information of any kind. No non-public personal information (NPPI) is necessary for purposes of performing services provided within the FICRAS system. No NPPI is required or permitted to be stored within the FICRAS system. The information gathered by FICRAS clients and stored for them, whether on FICRAS servers or the client's own servers is exclusively restricted to that client's use. Although FICRAS secures your data, only the client's authorized personnel control the information flowing through the client's FICRAS system. Each authorized user is given a personal access key. Their browser, IP and connection details are logged and matched against previous connections to ensure the highest level of confidence. FICRAS wants to know the person attempting to access the system is the correct person. All interaction is logged and histories are immediately available for monitoring secure usage of the system.

Security Incident Identification and Resolution Procedures:

If a system outage, service interruption, unauthorized use, password compromise, or any other system issue is identified by any authorized client, provider, contributor or administrator of the DAC-FICRAS Service System they are directed to immediately notify the following DAC-FICRAS authorized representatives.

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Robert Fitzpatrick, Webtent Networking - DAC-FICRAS System Security Agent
Email: webmaster@webtent.com

Disaster Recovery Policy and Procedures:

Disaster Recovery Policy Statement:

Upon receipt of a disaster notification, a support ticket will be created within the WebTent Networking Support Help Desk accessed at: https://www.webtent.net/support/ticket/index.php. The support ticket will form the communication basis through which incident identification, tracking, monitoring, and resolution will take place. Once resolution is complete, affected authorized users are to be identified and a complete incident report is to be logged for future reference and distributed to affected authorized users. The report will identify the date and time of the incident, the type of incident, the process used to identify the incident, the steps taken to resolve the incident, the date and time the incident was resolved, and what steps are being taken to ensure the incident does not reoccur. The final resolution report will be submitted to the DAC-FICRAS Services Administrator who will then determine if the incident has been adequately resolved and this report will be transmitted to the DAC Executive Committee for final consideration and determination with regard to modifications that may be required to ensure the incident does not reoccur.

It is the policy of the DAC-FICRAS Service System to ensure that any disaster downtime that may occur will result in as short a period as possible regarding the provision of services and data security to clients, providers, contributors, administrators, and all others that are authorized users of the DAC-FICRAS Service System.

POLICY AND PROCEDURES: (Continued)

Disaster Recovery Policy and Procedures: (Continued)

Disaster Recovery Policy Statement: (Continued)

Disaster Recovery Consideration and Prevention - The DAC-FICRAS Service System, its applications and data are routed, secured, and maintained within the WOW Enterprises, LLC (WOW) network operation center (NOC) located in Tampa, FL. WOW is a Type II certified data center system with redundant locations. According to WOW, "Our Tampa Data Center is designed to meet the most rigorous uptime and security standards. It features a dedicated, three-megawatt power substation, served by redundant power grids, bunker-grade architecture, and best-in-class infrastructure. The Tampa Data Center provides N+1 Redundancy, HIPAA, and PCI Compliant Facilities to keep your critical data available to you and your customers through the most extreme circumstances". [Learn More] All DAC-FICRAS Service System network servers are co-located within the WOW NOC and are professionally managed under agreement with WebTent Networking, Inc. WebTent has provided service without major incident for DAC-FICRAS since its inception.

It is highly unlikely that a disaster recovery need will occur; however, the DAC-FICRAS Service System is prepared for this eventuality. We maintain redundancy, with daily backup of all operations and administrative files and activities, with hourly backup of data files. We maintain a full-time, real-time mirror backup of operations servers. If a disaster occurs, we are prepared to recover when the resources or infrastructure causing the disaster are restored.

Disaster Recovery Procedures:

All disaster incident report notifications are to be delivered immediately to:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Robert Fitzpatrick, Webtent Networking - DAC-FICRAS System Security Agent
Email: webmaster@webtent.com

The DAC-FICRAS Chief Technical Officer and the WebTent Networking representative will immediately assess the known disaster issues and report to the DAC-FICRAS Services Administrator and to the DAC Executive Committee Chair, their assessment and recovery recommendations. The required procedure shall ensure:

1) All data and application files are restorable and secure, and that no intrusion or corruption of the data has occurred.
2) That all server systems are restored as quickly as possible to full service or if partial service is restored, the level of the partial service so restored and the estimated time required facilitating complete service restoration.
3) Upon restoration of full services, the DAC-FICRAS Chief Technical Officer will file an incident report detailing the disaster occurrence, the reason, its start time, the duration of the disaster, its end time, steps taken to ensure data integrity, restoration procedures applied, and steps taken to ensure the same or similar disasters will not occur in the future.
4) Once the report is completed, it is to be filed with the DAC-FICRAS Services Administrator and the DAC Governance Executive Committee and is to be immediately communicated and distributed to all affected authorize clients, providers, contributors, and administrators.

Backup Policy and Procedures:

Backup Policy Statement:

It is DAC-FICRAS policy to provide the most comprehensive operations and administration data backup available in the marketplace. All DAC-FICRAS operations and data servers are to be redundant to ensure that "no loss" of critical operational or administrative data occurs. All administrative data are to be backed up daily, with operational data backed up hourly. The DAC-FICRAS Service System shall maintain redundant, mirror servers for both operations and

Backup Policy Statement: (Continued)

development as may be needed to ensure backup of data is made between these servers in real time.

Backup Procedures:

The officers and consultants responsible for ensuring complete backup of all DAC-FICRAS data are:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Robert Fitzpatrick, Webtent Networking - DAC-FICRAS Service System Webmaster and Security Agent
Email: webmaster@webtent.com

The officers and consultants responsible for DAC-FICRAS data backup will:

1) Monitor backup activities within the DAC-FICRAS Service System to ensure the backup plan includes, at a minimum, the equipment and activities required to produce required backup consistent with the DAC-FICRAS Service System Backup Policy Statement referenced herein.
2) Log all backup procedures and processes that occur and review said logs to ensure the planned backup times referenced are being adhered to and report any issues affecting data backup to the DAC-FICRAS Services Administrator and will consult with said administrator to determine any modifications required to facilitate system and data backup consistent with the Backup Policy Statement, referenced herein.

Data Classification Policy and Procedures:

Data Classification Policy Statement:

All DAC-FICRAS associates, contractors, clients, providers, contributors, and any other authorized user of the DAC-FICRAS Service System who come into contact with sensitive *DAC-FICRAS or DAC-FICRAS financial institution client* internal information are expected to familiarize themselves with this data classification policy and to consistently follow the procedures outlined when such information is encountered. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, IS employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications. The types of information that may be permitted to be contained in the DAC-FICRAS Service System are classified as follows:

RESTRICTED Information - This classification applies to the most sensitive business information that is intended for use strictly by authorized DAC-FICRAS operations and administrative personnel or any authorized client of the DAC-FICRAS Service System. The unauthorized disclosure of “Restricted” information could seriously and adversely impact DAC-FICRAS operations and administration or any client of the DAC-FICRAS Service System, including their customers and authorized service providers.

CONFIDENTIAL Information - This classification applies to less-sensitive business information that is intended for use within the DAC-FICRAS Service System Its unauthorized disclosure could adversely impact DAC-FICRAS operations and administration or any client of the DAC-FICRAS Service System, including their customers and authorized service providers.

PUBLIC Information - This classification applies to information that has been approved by DAC-FICRAS Services Administrator for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

POLICY AND PROCEDURES: (Continued)

Data Classification Policy and Procedures: (Continued)

Information Ownership and Access Decisions – All DAC-FICRAS clients and providers are made aware of the DAC-FICRAS "**No Non-Public Personal Information (NPPI)**" data management policy. The DAC-FICRAS Service System does not require any NPPI to conduct its business. Therefore, each client is notified as part of DAC-FICRAS Service System license agreement that no NPPI is to be gathered, stored, or distributed into or out of the DAC-FICRAS Service System and to do so would be a material breach of that client's or provider's DAC-FICRAS license agreement. Each financial institution (FI) client owns their respective data developed as a result of their operations within their DAC-FICRAS Service System. Along with data ownership, each client controls access to their various DAC-FICRAS data components through their own IT department representative who administers that client's information access authorization processes. The DAC-FICRAS Service System provides the ability for each FI client to control and administer their own access and each FI client is individually responsible for their own policy and procedures to be used in managing their sensitive data. FI client personnel who are responsible for that client's information access are provided training and support in the DAC-FICRAS Service System procedures established that enable them to control access to their own data environment.

Data Classification Procedures:

The responsibility for data classification oversight for information pertaining to DAC-FICRAS Service System operations and administration rests with the following DAC-FICRAS officers:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com

Any DAC-FICRAS data classification issue or question pertaining to data disclosure, authorized access to data or other classification related issues are to be immediately transmitted to the DAC-FICRAS responsible officers identified above. Upon receipt the officers will review the issue or question, make inquiries as necessary pertaining to them and prepare a report of their findings and deliver said report to any affected authorized user within the system to ensure the maintenance of data is consistent with this data classification policy. The findings report will be filed with the DAC Governance Committee once resolved to determine if data classification policy and procedures need modification or revision. The DAC Governance Executive Committee shall make the final determination and report their findings back to the responsible officers. If it is found that the data classification policy and/or procedures require modification, the responsible officers will then move to make such modification and submit the modified data classification policy statement and procedures to the DAC Governance Executive Committee for final approval. Once approved, the modified policy and procedures will be published and distributed to all affected DAC-FICRAS personnel and FI clients.

Privacy Policy and Procedures:

Privacy Policy Statement:

In the course of conducting its business, the DAC-FICRAS Service System gathers certain information required to facilitate the operations of the DAC-FICRAS Service System and the lawful applications of its clients in their authorized use of the system. It is the DAC-FICRAS Service System policy to never share, sell, trade, or otherwise distribute any information to third parties regarding any individual or organization authorized to use the DAC-FICRAS Service System, whatsoever, except with regard to DAC-FICRAS Service System marketing as may be authorized individually in writing by clients and other authorized users of the system.

POLICY AND PROCEDURES: (Continued)

Privacy Policy and Procedures: (Continued)

Privacy Procedures:

The foregoing policy prohibits the sharing of information pertaining to users and/or use of the DAC-FICRAS Service System. Any question pertaining to the DAC-FICRAS Service System privacy policy shall be directed to the following responsible officer for determination:

> Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
> Email: administration@ficras.com

Upon receipt of any inquiry, the responsible officer will investigate the issue, gather sufficient information for final determination and will report back to the inquiring party the result of that investigation. Once the question is resolved, the responsible officer shall report the inquiry, the investigation and solution results to the DAC Governance Executive Committee for determination if the privacy policy and procedures require modification. If so, the responsible officer will make modifications as directed by the DAC Executive Committee and will provide them a copy of the modified policy and or procedure whichever may be the case and the policy and/or procedure so modified will become a part of the DAC-FICRAS Policy and Procedures going forward. All affected constituents of the DAC-FICRAS service system will then be notified of the modifications as required to ensure compliance with the DAC-FICRAS Service System privacy policy.

Confidentiality Policy and Procedures:

Confidentiality Policy Statement:

All officers, employees, associates, contractors, providers and their employees, if any, serving the DAC-FICRAS Service System, its authorized clients, providers, contributors, and administrators are bound by ethical and legal codes to protect the confidentiality and privacy of every authorized user interfacing with the system. It is the duty of all user constituents to protect and maintain the confidentiality of all information learned about clients, their operations, their clients, providers, contributors and administrators in the course of providing DAC-FICRAS services to them. Confidential communications include conversations, reports, forms, correspondence, and computer generated communications with, about or involving in any way any client of the DAC-FICRAS Service System. Minors are entitled to confidentiality also, and only the guardian of the minor can waive the confidentiality. Access to documentation shall be limited to an “as needed/need to know” basis and shall not be disseminated in any format without the prior written authorization of the DAC-FICRAS Services Administrator. Any breach of confidential information of any kind within the DAC-FICRAS Service System is a top priority concern and is to be managed post haste to resolution.

Confidentiality Procedures:

The DAC-FICRAS Service System responsible officer regarding all confidentiality issues is:

> Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
> Email: administration@ficras.com

Confidentiality questions or issues identified will be immediately directed to the responsible officer identified above. In the event a breach of confidentiality incident is suspected to have occurred, the responsible officer shall investigate the facts of the case, gather necessary information to examine the facts and make a determination if in fact a confidentiality breach has occurred. If it is determined a breach has occurred, the responsible officer will identify the source of the breach and take whatever steps are necessary to eliminate the potential for said breach to continue. The goal in the event of an unauthorized confidentiality breach is to minimize the damage of said breach. Once the necessary steps are taken to eliminate the confidentiality breach threat, the responsible officer shall prepare a report for submission to the DAC Executive Committee for review and final recommendation. Once received, the responsible officer will proceed to finalize all the issues in accordance with the DAC Executive Committee recommendation and shall report the results of such efforts to close that incident. Once resolved the responsible officer shall report all pertinent information to all affected authorized users identified in the investigation and will file a final report of resolution with the DAC Governance Executive Committee for further action, if any.

POLICY AND PROCEDURES: (Continued)

Acceptable Use Policy and Procedures:

Acceptable Use Policy Statement:

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by any DAC-FICRAS Service System constituent or a third party. All authorized user constituents are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, laws and regulation. This policy applies to all DAC-FICRAS Service System employees, contractors, consultants, contributors, clients, their providers and others that may be authorized to use the system. This policy applies to all equipment that is owned or leased by the DAC-FICRAS operating entity, its employees, contractors, consultants, contributors, clients, their providers, contractors and their employees, if any.

General Use and Ownership of Information:

Proprietary information stored on electronic and computing devices whether owned or leased by the DAC for use in recording, storing or distributing proprietary information or if said devices are owned by an employee, associate, contractor, provider, contributor or other third party, remains the sole property of the DAC-FICRAS Service System. Each constituent having access to said proprietary information must ensure through legal and technical means that proprietary information is protected in accordance with the Acceptable Use Policy Statement, including the following:

1) You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.
2) If authorized by the DAC-FICRAS Services Administrator or other DAC-FICRAS designated authority authorized to approve said access, you may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned duties within the system.
3) All authorized constituents are responsible for exercising good judgment regarding the reasonableness of personal use.
4) If there is any uncertainty regarding the access to or use of proprietary information, personnel having such questions are directed to immediately contact the DAC-FICRAS Services Administrator for guidance before proceeding with any activity where proprietary information is concerned.
5) For security and network maintenance purposes, authorized DAC-FICRAS Service System personnel may monitor equipment, systems and network traffic at any time to ensure proper care and security of the proprietary information.
6) Administrators of the DAC-FICRAS Service System operations reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security of Proprietary Information:

All mobile and computing devices that connect to the internal network must comply with the authorized access policy that may from time to time be adopted, modified or enacted either by a responsible officer so authorized by the DAC Executive Committee or in the absence of such officer, by the DAC-FICRAS Services Administrator. All activities must comply with the following:

1) System level and user level passwords must comply with the Password Policy.
2) Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
3) All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
4) No postings by authorized personnel from an email address to newsgroups shall be made, except those so authorized for marketing and informational purposes and all such postings shall be approved by the DAC-FICRAS Services Administrator or other designated constituent as may be authorized directly by the DAC Executive Committee. Any such posting shall contain appropriate disclaimer language regarding the postings as may be approved from time to time by the designated DAC-FICRAS Service System authorized personnel as may be appointed by the DAC Executive Committee.
5) All personnel must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. If any suspicious e-mail is received by personnel, they are to notify the DAC Services Administrator immediately for resolution.

POLICY AND PROCEDURES: (Continued)

Acceptable Use Policy and Procedures: (Continued)

Unacceptable Use of Proprietary Information:

The following activities are, in general, prohibited. DAC-FICRAS Service System personnel may be exempted from these restrictions during the course of their legitimate job responsibilities, subject to the written authorization by the DAC-FICRAS Services Administrator or the DAC Executive Committee as directed authorization may be proscribed. All authorized DAC-FICRAS personnel shall be subject to the following:

1) Under no circumstances are any personnel, clients or their employees, contractors, contributors or providers authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the DAC-FICRAS Service System or the resources available through that medium.
2) The following system and network activities are strictly prohibited, with no exceptions:
   a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the DAC-FICRAS Service System.
   b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which or the end user does not have an active license is strictly prohibited.
   c. Accessing data, a server or an account for any purpose other than conducting business, even if you have authorized access, is prohibited.
   d. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The DAC-FICRAS Services Administrator or other representative so authorized by the DAC Executive Committee should be consulted prior to export of any material that is in question.
   e. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
   f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
   g. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
   h. Making fraudulent offers of products, items, or services originating from any account.
   i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
   j. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the constituent(s) is/are not an intended recipient or logging into a server or account that the constituent is not expressly authorized to access, unless these duties are within the scope of regular duties appropriately authorized for that constituent to conduct. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
   k. Port scanning or security scanning is expressly prohibited unless prior notification authorization is received in writing from the DAC-FICRAS Services Administrator or other authority so authorized by the DAC Executive Committee.
   l. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
   m. Circumventing user authentication or security of any host, network or account.
   n. Introducing honeypots, honeynets, or similar technology on the network.
   o. Interfering with or denying service to any user (denial of service attack).
   p. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
   q. Providing information about, or lists of DAC-FICRAS Service System authorized personnel, including employees, contractors, providers, contributors, FI clients, their clients, employees, contractors, providers, etc. to parties outside the DAC-FICRAS Service System unless so authorized by the DAC-FICRAS Services Administrator or other authority so authorized by the DAC Executive Committee.

POLICY AND PROCEDURES: (Continued)

Acceptable Use Policy and Procedures: (Continued)

Email and Communication Activities:

When accessing the Internet for purposes of DAC-FICRAS Service System business, users must realize they represent the company. Whenever an authorized DAC-FICRAS Service System constituent states an affiliation to the company, they must also clearly indicate, unless otherwise authorized as part of their official capacity, that "the opinions expressed are their own and not necessarily those of the company". Questions regarding internet use restrictions should be addressed to the DAC-FICRAS Services Administrator or other authorized representative as may be appointed by the DAC Executive Committee.

The following are email and communication activities that are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within networks of other Internet/Intranet/Extranet service providers on behalf of the DAC-FICRAS Service System or to advertise any service hosted by or connected via the DAC-FICRAS Service System network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media Activities:

Blogging by employees, whether DAC-FICRAS property or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Occasional use of systems to engage in blogging is acceptable following receipt of written approval as may be presented ty the DAC-FICRAS Services Administrator or others so authorized by the DAC Executive Committee. Any authorized blogging activities are to be done in a professional and responsible manner, Each authorized constituent who participated in blogging on behalf of the DAC-FICRAS Services System must ensure that their activities do not otherwise violate this policy and that said blogging activity will not be detrimental to the system's best interests. No blogging activity shall interfere with any constituent's regular work duties. Authorized blogging from the DAC-FICRAS Service System is subject to:

1. Monitoring.
2. Confidential Information policy also applies to blogging. As such, authorized constituents are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by the Confidential Information policy when engaged in blogging.
3. No constituent shall engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of and/or any of DAC-FICRAS services system authorized user constituents.
4. No discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by law.
5. Constituents may not attribute personal statements, opinions or beliefs to the DAC-FICRAS Service System when engaged in blogging.
6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, DAC-FICRAS Service System trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity.

POLICY AND PROCEDURES: (Continued)

Acceptable Use Policy and Procedures: (Continued)

Acceptable Use Procedures:

Any question regarding acceptable use of DAC-FICRAS Service System media shall be directed to:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

Vulnerability Management Policy and Procedures:

Vulnerability Management Policy Statement:

This policy applies to vulnerability management policy and controls required to maintain high levels of system and application security. It outlines the technology and procedures necessary for implementing a comprehensive, integrated program to detect and remediate vulnerabilities in operating systems, applications, mobile devices, cloud resources, and network devices to maintain maximum levels of security pertaining to services delivered through the DAC-FICRAS Service System.

The following vulnerability management procedures are to be followed until modified as may be needed in the future.

1) The DAC-FICRAS Service System responsible officers and consultants for execution of vulnerability management policy and procedures (Vulnerability Team) are:
   Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
   Email: support@ficras.com
   Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
   Email: administration@ficras.com
   Robert Fitzpatrick, Webtent Networking - DAC-FICRAS Service System Webmaster and Security Agent
   Email: webmaster@webtent.com
   Note: The officers and consultants identified may assign associates to form the Vulnerability Team as may be required in the course of their duties; however, any associate assigned to the Vulnerability Team must be approved in writing by the DAC Executive Committee prior to commencement of their participation in vulnerability testing and reporting.

2) The Vulnerability Team will establish, install and maintain as may be required on an on-going basis, a primary vulnerability assessment software solution to scan all DAC-FICRAS Service System infrastructure for devices on a scheduled periodic basis and will provide a report on the vulnerabilities identified across all assets to the DAC-FICRAS Services Administrator and the DAC Executive Committee.

3) Upon receipt of the reports, the Operations Team is responsible for:
   a) Reviewing the results;
   b) Providing a remediation via configuration changes or deploying security patches;
   c) Implementing other mitigating measures;
   d) Properly documenting any exceptions.

Vulnerability remediation is to be completed as soon as possible using the current Common Vulnerability Scoring System (CVSS) as published [https://www.first.org/cvss/] guidelines as follows:

POLICY AND PROCEDURES: (Continued)

Vulnerability Management Policy and Procedures: (Continued)

Vulnerability Management Policy Statement: (Continued)

Severity	Description	Service Level
Critical	Critical vulnerabilities have a CVSS score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits.	2 Days
High	High-severity vulnerabilities have a CVSS score of 8.0 or higher, or are given a High severity rating by PCI DSS v3. There is no known public malware or exploit available.	30 Days
Medium	Medium-severity vulnerabilities have a CVSS score of 6.0 to 8.0 and can be mitigated within an extended time frame.	90 Days
Low	Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can't be remediated.	180 Days

Any findings that need to be mitigated later than the service level must be approved by the DAC-FICRAS Services Administrator. The findings are to be documented as exceptions and filed for review by the DAC Executive Committee. Team members may also use specialized scanners to identify specific vulnerabilities or gain a deeper level of analysis, such as the Retina Web Security Scanner, FireEye, SourceFire, etc.

Vulnerability Scan Targets include all devices connected to both public and private segments of the network. Device scans are organized by the individually defined address spaces, active directory queries, cloud resources, and locally installed agents or other characteristics as may be determined to be appropriate by the Vulnerability Team. These are referred to as "User Groups" in this document.

Vulnerability Management Procedures:
A User Group specifies a collation of hosts to be scanned and is named for the "commonality" that it holds for assets. A User Group name also identifies its classification or a general description of the hosts/devices on the network, and is used for role-based access for team members to restrict unauthorized access. A new User Group can be established, or an existing one changed, by submitting a request to the DAC-FICRAS Services Administrator.

Upon receipt of a vulnerability management request, the Vulnerability Team will conduct the vulnerability management procedures outlined previously.

Vulnerability Scan Frequency:

The DAC-FICRAS Chief Technical Officer shall establish the scan frequency scheduling in accordance with best practices and will report such scan frequency periods to the Vulnerability Team who will then provide scanning in accordance with the schedule as it may be established from time to time. The schedule will include:

1) All server and sensitive host scans;
2) All desktop and other scans;
3) New asset discovery scans;
4) All new assets to be included as production for desktops or servers;
5) All software operating systems on the network devices (routers, switches, VPN, firewalls, wireless, and DNS/DHCP;
6) Individual system scans may be performed at any time.

POLICY AND PROCEDURES: (Continued)

Vulnerability Management Policy and Procedures: (Continued)

Vulnerability Reporting:

The Vulnerability Team will report their vulnerability assessment activities on a regular time schedule as may be directed by the DAC Executive Committee. The Vulnerability Team members responsible for reporting are:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

The DAC-FICRAS Services Administrator may designate or otherwise authorize an alternate Vulnerability Team member as may be directed by the DAC Executive Committee from time to time to provide reporting services. All vulnerability management reports will be delivered to the DAC-FICRAS Services Administrator and to the DAC Executive Committee for review, consistent with the reporting frequency established by that committee to ensure proper oversight of all Vulnerability Management activities within the DAC-FICRAS Service System.

Change Management Policy and Procedures:

Change Management Policy Statement:

Changes to the DAC-FICRAS Service System must follow a structured process to ensure appropriate planning and execution. The Information Technology Infrastructure Library (ITIL) defines three types of changes:

1) Standard Change - A repeatable change that has been pre-authorized by the Change Authority by means of a documented procedure that controls risk and has predictable outcomes.
2) Normal Change - A change that is not an Emergency change or a Standard change. Normal changes follow the defined steps of the change management process. Low, Medium, or High priority as may be determined.
3) Emergency Change - A change that must be introduced as soon as possible due to likely negative service impacts. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps due to the urgent nature of the issue.

Change Management Procedures:

The DAC-FICRAS Service System officer(s) responsible for Change Management are:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

For FICRAS:
Cheryl Bella, MAI, AI-GRS DAC-FICRAS Chief Compliance Officer
Email: cbella@ficras.com

The responsible officers may from time to time assign change management oversight to other DAC-FICRAS Service System personnel as may be required in the course of their duties. The officer(s) responsible, together with those personnel assigned to implement change management policy are hereafter referred to as the Change Management Team.

When changes are identified, the Change Management Team will be notified. The Change Management Team will then assess the prospective change to determine the type of change as described above. Standard changes may be undertaken and directed by the Change Management Team, following approval of the responsible officer(s) as may be established from time to time. For changes identified as Normal, the Change Management Team will identify the priority of the change (Low, Medium or High) and will lay out a procedural map that the Change Management Team will follow in the orderly process of effecting such change in accordance with the priority established. Any changes identified as Emergency are by definition of the highest priority and are to be immediately effected by the Change

POLICY AND PROCEDURES: (Continued)

Change Management Policy and Procedures: (Continued)

Change Management Procedures: (Continued)

Management Team. Upon completion of any ITIL identified change, the Change Management Team will file a report detailing the type of change, the effect of the change on the DAC-FICRAS Service System, the change procedures followed, the testing procedures followed in effecting the change and the date and time the change was released for general use. Irrespective of whether or not ITIL changes have taken place during the reporting period, the responsible

Change Management Team member shall file a report, at least ***quarterly*** at the beginning of each calendar quarter, if required, detailing the activities of the Change Management Team during that quarter. For change types identified as Normal and Emergency, the Change Management Team shall notify and obtain written permission from the DAC-FICRAS Services Administrator prior to or immediately after the change being effected within the system. The change priority will determine the change report delivery timing as may be determined to be appropriate by the supervising Change Management Team member assigned by the DAC-FICRAS Services Administrator.

Incident Response Policy and Procedures:

Incident Response Policy Statement:

Although no Non-Public Personal Information (NPPI) of any kind is required for operation of services within the DAC-FICRAS Service System, a security incident response capability will be developed and deployed for all information systems that house or access DAC-FICRAS Service System controlled information. This shall include any confidential information used as part of the operation of each client's DAC-FICRAS Service System. The incident response capability will include a defined plan and will address the seven stages of incident response, including preparation, detection, analysis, containment, eradication, recovery, and post-incident activity. Preparation includes development and deployment of an Incident Response Team to enable the effective administration of the incident response policy. The DAC-FICRAS Service System Incident Response Team responsible officers and consultants are:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Robert Fitzpatrick, Webtent Networking - DAC-FICRAS Service System Webmaster and Security Agent
Email: webmaster@webtent.com

The responsible officers may from time to time assign incident response management oversight to other DAC-FICRAS Service System personnel as may be required in the course of their duties. The officer(s) responsible, together with those personnel assigned to manage incident response policy are hereafter referred to as the Incident Response Team.

The DAC-FICRAS Service System Incident Response Team shall establish, implement, monitor, and report their activities to the DAC Executive Committee as may be required to affect oversight and compliance with this policy.

Incident detection protocols shall be in compliance with computer emergency response team (CERT) coordination center (CERT/CC) for the Software Engineering Institute (SEI), a non-profit United States federally funded research and development center. The CERT/CC researches software bugs that impact software and internet security, publishes research and information on its findings, and works with business and government to improve security of software and the internet as a whole.

Incident Response Procedures:

Upon detection of a potential intrusion incident, any authorized user of the DAC-FICRAS Service System will immediately report said incident by email to:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

POLICY AND PROCEDURES: (Continued)

Incident Response Policy and Procedures: (Continued)

Incident Response Procedures: (Continued)

Following receipt of a potential intrusion incident, the DAC-FICRAS Service System Incidence Response Team shall:

1) Analyze the reported intrusion and research any report of related intrusions within the CERT/CC knowledge database [https://www.sei.cmu.edu/about/divisions/cert/index.cfm]. Make a determination if the intrusion is a known attempt and if not, report same to the CERT/CC system for followup. Will determine in the analysis, the level of intrusion, the method of intrusion, the time period of the intrusion, and the data affected by the intrusion.
2) Contain the intrusion so identified to prevent further incident.
3) Eradicate the intrusion capability, to include modification of software code, access procedures or any other vulnerability identified.
4) Recover data loss, if any, affected by the incident.
5) Post-Incident activity will include report followup with the CERT/CC, detailing all the findings regarding the incident and coordinating with the CERT/CC any further followup that would enhance intrusion monitoring in the future. Preparing a complete “Incident Report” detailing the CERT/CC activities undertaken regarding the incident, the procedures followed in detecting and analyzing the incident, the containment and eradication activities employed in response to the incident, and the data recovery processes implemented to effect restoration of any data that may have been compromised as a result of the incident.

Critical Incident Management Policies and Procedures:

Critical Incident Policy Statement:

A critical incident is an unexpected traumatic event, involving personal or professional threat, which evokes extreme stress, fear or injury. Providing appropriate supports following a critical incident is part of emergency management. The DAC-FICRAS Service System Critical Incident Policy is established to provide immediate response to any critical incident identified and to support DAC-FICRAS Service System authorized users during and following a critical incident. For this purpose, the DAC-FICRAS Service System officers and consultants responsible for critical incident management are:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Robert Fitzpatrick, Webtent Networking - DAC-FICRAS Service System Webmaster and Security Agent
Email: webmaster@webtent.com

The DAC-FICRAS Service System responsible officers shall prepare a Critical Incident Response Plan (CIRP) that is consistent with best practices. The plan shall include at a minimum:

1) Establishment and implementation of a Critical Incident Response Team (CIRT)
2) The critical incident identification and reporting processes to be undertaken by DAC-FICRAS Service System support personnel, clients, providers, administrators and all authorized users of the system in the event of a critical incident.
3) A critical incident report receipt procedure that is to be followed, further outlining the information to be gathered regarding the critical incident.
4) The CIRP shall include provisions for emergency coordination of services for injury to any person as a result of the critical incident.
5) The CIRP shall include provisions for immediate protection of all software, hardware, connectivity, and data assets of the DAC-FICRAS Service System, with special regard to all client data client operations that may be affected by the critical incident.
6) A monitoring plan to ensure information regarding the critical incident response is made available for later reporting purposes.
7) A critical incident debriefing (CID) procedure that will enable recovery from the critical incident exposure in the shortest period of time.

POLICY AND PROCEDURES: (Continued)

Critical Incident Management Policies and Procedures: (Continued)

Critical Incident Procedures:

Upon receipt of a critical incident notice the Critical Incident Response Team (CIRT) will immediately:

1) Notify all affected constituents of the DAC-FICRAS Service System of the critical incident, detailing:
   a) The nature and severity of the incident;
   b) If it is a physical incident, the safest route of escape available to those affected by the incident;
   c) If it is a technical or operational incident, the steps to be taken by each authorized constituent to minimize the identified damage that could potentially result from the critical incident.
2) Notify all emergency management services that can be called upon to assist with the critical incident management response and direct them to the location of the reported incident.
3) Monitor the progress of the critical incident response and expedite any additional response that may be required to mitigate or eliminate the critical incident threat.
4) Report the results to the designated CIRT leader, detailing:
   a) The nature and severity of the incident;
   b) If it was a physical incident, the instructions provided by the CIRT regarding safest route of escape available to those affected by the incident;
   c) The emergency management procedures followed as required of best practices regarding the deployment of emergency management services and how the emergency management response was monitored and coordinated during and after the incident;
   d) If a technical or operational critical incident, the instructions provided to affected constituents, the steps taken by each authorized constituent to minimize the potential critical incident damage and the monitoring processes utilized to ensure that each constituent followed the instructions provided;
   e) The steps taken to ensure compliance with all critical incident instructions communicated to authorized constituents and the identity of constituent authorized users who either intentionally or inadvertently did not comply.
   f) The CID procedure undertaken to enable recovery;
   g) The level of anticipated recovery;
   h) The on-going critical incident recovery mitigation steps that should continue to be taken.
   i) The steps and processes that need to be undertaken to minimize the effect of a similar critical incident in the future.
   j) Updates required to the Critical Incident Policy and Procedures as well as other DAC-FICRAS policy and procedures as may be required based on the experience of critical incidence exposure.
5) Report all findings to the DAC-FICRAS Services Administrator and the DAC Executive Committee for final review, recommendations and policy/procedure modifications as determined to be appropriate, if any.

Performance Management Policy and Procedures:

Performance Management Policy Statement:

The DAC-FICRAS Service System cultural environment supports performance management, guided by the recognition that performance management is an on-going human behavioral process, often involving peer and supervisory coaching, mentoring, and motivating to secure the optimal result for all affected team members. It is recognized, effective performance management leads to enhanced productivity, performance and job satisfaction. It is also recognized that the process of addressing poor performance or problematic behaviors need to be transparent and rooted in correcting the identified deficiencies with alternatives to ensure the most favorable outcome possible that is available to each team member.

The DAC-FICRAS Service System responsible officer for oversight regarding adherence to this policy is:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

POLICY AND PROCEDURES: (Continued)

Performance Management Policy and Procedures: (Continued)

Performance Management Procedures:

All DAC-FICRAS Service System activities are project oriented and assigned to project teams. A project team consists of an authorized team leader (ATL), together with personnel that may provide direct or indirect support to the ATL in achieving the project team goals. The ATL is the point of focus for performance management activities among his/her support group and the support group is the point of focus for performance management activities among the ATL's they serve in a project. For purposes of identification herein, all team leaders and team members are referred to as "constituents"

A performance audit of all constituents shall be performed at least once annually and preferably quarterly among the various ATL's and support team groups. Each constituent will receive copies of performance audit reports related to their activities. The performance audit standard report is still in development but will be provided to all constituents once finalized. All performance audit reports are to be held in strict confidence and only made available to the constituent it involves, the oversight officer identified, and the DAC Executive Committee as required to perform their duties with regard to performance management.

The performance management of each constituent is subject to a performance audit within the DAC-FICRAS Service System. At the beginning of the performance management cycle, an audit package (still under development) shall be delivered to the oversight officer identified for determination of performance levels provided by that constituent. The constituent will be notified by the oversight officer and the applicable components of the audit package that are to be delivered to the constituent shall be delivered to them.

Each constituent shall be provided a self-evaluation form to conduct an audit of their own activities and behaviors in performing their duties. These will then be combined in a confidential meeting to discuss the performance of the constituent, their aspirations and comfort levels within the organization and the opportunities they perceive as being present as well as what changes they would affect in the organizational structure or operating environment they find themselves in. From the meeting, notes of performance improvements and enhancement procedures will be made and an agreement regarding the constituent's future performance, their training and education needs, their service and behavioral enhancement options in an effort to set a performance management standard for that constituent, with an eye to maximizing his/her effectiveness and creating an atmosphere of success in the services they perform.

This process will be transparent between the constituent and the oversight officer and will be confidential in all respects. Any officer, ATL or support team group member who breaks the confidentiality of any performance management activity, especially performance audits and their results, shall be subject to immediate reprimand and ultimately dismissal as may be directed by the DAC Executive Committee. Through this process, it is anticipated that all constituent's performance can be fairly audited as a result. The goal is to seek agreed upon enhancement options that can be adopted to maximize the value of the constituent to the DAC-FICRAS Service System and vice-versa.

Asset Management Policy and Procedures:

Asset Management Policy Statement:

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

For assets adapted to serve the DAC-FICRAS Service System, the following minimal asset classes are subject to tracking and asset tagging:

1) Desktop workstations
2) Laptop mobile computers

Asset Management Policy and Procedures: (Continued)

Asset Management Policy Statement: (Continued)

3) Tablet devices

4) Printers, copiers, fax machines, and multifunction print devices

5) Handheld devices

6) Scanners

7) Servers

8) Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)

9) Private Branch Exchange (PBX) and Voice over Internet Protocol (VOIP) Telephony Systems and Components

10) Internet Protocol (IP) Enabled Video and Security Devices

11) Memory devices

Asset Value:

Assets which cost less than $500.00 shall not be tracked, including computer components such as smaller peripheral devices, video cards, or keyboards, or mice. However, assets, which store data regardless of cost, shall be tracked either as part of a computing device or as a part of network attached storage. These assets include:

Network Attached Storage (NAS), Storage Area Network (SAN) or other computer data storage

Temporary storage drives

Tape or optical media with data stored on them including system backup data

Asset Management Procedures:

The DAC-FICRAS Service System responsible officer for asset management policy is:

Natalie D. Hill, DAC-FICRAS Finance Director
Email: finance@ficras.com

The responsible officer shall establish procedures in accordance with this policy to track all assets that are subject to asset tracking and reporting and shall provide the DAC-FICRAS Services Administrator a copy of said procedures to submit to the DAC Executive Committee for approval.

Password Management Policy and Procedures:

Password Management Policy Statement:

Effective password management is foundational to protecting against unauthorized access to the DAC-FICRAS Service System. All constituents are notified hereby that it is their responsibility as an authorized user of the system to take whatever steps are necessary to protect their password for authorized use of the DAC-FICRAS Service System. It is the policy that any breach of password protocols by any constituent, now or in the future, is prohibited and that any recognized or potential breach of the password protocols and procedures called for in

Password Management Policy Statement: (Continued)

support of this policy is sufficient reason for that constituent to be barred from further use of the DAC-FICRAS Service System.

The responsible officers for all password management policy compliance are:

Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

Password Management Procedures:

The responsible officers will establish password management procedures that ensure:

1) Each potential user constituent is made aware of the password management protocols so established by the responsible officers and approved by the DAC Executive Committee.

2) Monitoring of password protocol compliance is conducted on a regular basis (not to exceed three (3) months).

3) A password compliance tracking system is prepared and adopted for all authorized user constituents.

4) Best practices password strength protocols established are appropriately communicated and strictly adhered to by all authorized user constituents.

5) All authorized user constituents are made aware of and correctly employ password security procedures (non-sharing of passwords, etc.);

6) All authorized user constituents are aware of established or yet to be established reminder systems used to notify them when it is time to modify their password, consistent with best practice security policy;

7) All authorized user constituents regularly modify their passwords consistent with reminder system time periods;

8) Any authorized user constituent that does not comply to the password management procedures is identified and warned regarding their non-compliance; and

9) A password compliance resolution plan is established for authorized user constituents who consistently are not in compliance with password.procedures that may from time to time be adopted in keeping with the password management policy that may from time to time be modified by the responsible officers and approved by the DAC Executive Committee.

Onboarding Process Policy and Procedures:

Onboarding Process Policy Statement:

This policy governs the onboarding and orientation processes and sets out roles and responsibilities to ensure all new associates, independent contractors and other contributors, together with DAC-FICRAS Service System clients feel welcome and are apprised of the policy and procedures affecting their use of the DAC-FICRAS Service System as a team member and that the organization minimizes the time required for each participant to become a contributing team member or client participant.

POLICY AND PROCEDURES: (Continued)

Onboarding Process Policy and Procedures: (Continued)

Personnel Onboarding Procedures:

The DAC-FICRAS Service System responsible officer for oversight of the onboarding process policy is:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

All new hires will be required to undergo a thorough background check and will sign an authorization for the DAC FICRAS responsible officer to conduct background research on each new hire as deemed necessary by the responsible officer to ensure the new hire's ability to perform the services required.

The onboarding procedures shall include the following at a minimum: new hires, whether engaged as employees, independent contractors or under other arrangements (personnel leasing, etc.) shall be provided a new hire packet which will contain:

1) A welcome package detailing the DAC-FICRAS Service System organization structure, culture, operating history, general business plan, opportunities, benefits and expectations of provider and contributor constituents of the service system.

2) An introduction to the resources available to the constituent.

3) A complete description of the functions the constituent will be expected to perform under the engagement.

4) An overview of the importance system security plays in the operation of the system and the policies and procedures the constituent must adhere to in conducting his/her services.

Each new hire will receive assignment of a mentor who will assist the constituent in becoming familiar with his/her new surroundings, their duties and will introduce them to other team members that they may be working with. If the constituent's services are to be performed off-site the mentoring and introduction process will be conducted in an on-line meeting, with screen camera introductions so that remote constituents have an opportunity to be introduced to the team management environment and the probable project team members they will be working with as part of the DAC-FICRAS Service System operations. At the end of the new hire constituent's first week of service, the assigned mentor will interview the constituent to determine any additional adjustment needs they may have and will assist them in obtaining solutions to those needs, either by direct provision from system resources or by special request to the authorized officer identified. This process will be repeated again at the end of the constituent's first month of service.

Client Onboarding Procedures:

DAC-FICRAS Service System clients form the core of our business. As such, it is vitally important that each client receives direct assistance in system setup, training and ongoing support as they go through the process of implementation and adoption of the system in their day to day operations. The client onboarding team (COT) shall consist of the following responsible officers or their designees as may be appropriate:

Cheryl B. Bella, MAI, AI-GRS, DAC-FICRAS Chief Compliance Officer
Email: compliance@ficras.com
Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com
Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com

POLICY AND PROCEDURES: (Continued)

Onboarding Process Policy and Procedures: (Continued)

Client Onboarding Procedures: (Continued)

The DAC-FICRAS responsible officers shall set out a plan relevant to each new client to enable that client to move as rapidly as possible, consistent with the client's requirements, to complete the following processes:

1) System Introduction – The COT or delegate(s) as may be assigned shall provide either an on-line or in person demonstration of the DAC-FICRAS Service System to the client as may be appropriate in the context of familiarizing the client with the system.

2) Client Due Diligence – The COT or delegate(s) as may be assigned shall provide information as may be required by the client in determining their appropriate use of the DAC-FICRAS Service System as may be appropriate, keeping in mind that any confidential information provided to the client is maintained as "confidential" and proper notices are to be provided to the client regarding confidential information. Any client due diligence information requests are to be directed to the DAC-FICRAS Services Administrator who will be responsible for providing said information and the qualifications of the information provided will be clearly disclosed to the client. The primary emphasis in the due diligence process shall be transparency in every aspect of the information provided and it shall be the duty of the COT to ensure all requested or relevant information is provided to the client in a timely manner with all proprietary or confidential disclosures.

3) Client System Setup – The COT or delegate(s) as may be assigned shall assist the client's IT department in system setup, with full training and demonstration of the client's access controls to ensure the onboarding of client personnel can and will be as effortless and seamless as possible. Once system setup is complete, the COT will assist the client's IT department designated representative in testing the setup to ensure it is complete and that all setup procedures are followed and the client's IT designated representative shall be made aware of the COT personnel assigned to them and that those personnel will continue to be available to followup with any questions or activities that are required in the on-going process of DAC-FICRAS Service System use.

4) Client System Training – The COT or delegate(s) as may be assigned shall provide training to client personnel assigned to DAC-FICRAS Service System use. This will include lenders, appraisal review department (ARD), analysts, service providers, and others that may be presented to COT as authorized users of that client's system.

5) Client Support and Monitoring – The COT shall make known to the client, the communication and response processes that may be employed for immediate support as well as on-going support where immediate response is not required. In no event, shall a client request for support, once received, not be responded to within two (2) hours of its receipt. Ideally, the response time should less than one (1) hour; however, client support response time is a high priority function of the COT. The COT from time to time will administratively monitor client activities to ensure that their DAC-FICRAS Service System operations are performing at optimal levels with regard to the types of services being processed through the client's system and that the client's activities are consistent with the security policy of the system in general.

Termination Process Policy and Procedures:

Termination Process Policy Statement:

The DAC-FICRAS Service System will observe all legal requirements referring to termination/separation of personnel engagements whether by employment agreement, independent contractor agreement or other services employment type and will avoid "implied contracts" and unnecessary terminations.

The DAC-FICRAS Services System responsible officer for termination process policy is:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

Termination Procedures:

Voluntary Termination:

Voluntary termination can be the result of resignation, retirement, failure to show for work for a specified number of days, and expiration or completion of a contract for services. If voluntary termination occurs, the terminating constituent's project team leader (PTL) shall notify the designated responsible officer in writing and will identify the conditions under which the constituent's termination occurred. If required, the responsible officer or their designee as may be appropriate shall file any notices required and will comply with all regulatory requirements applicable to the engagement agreement under which the terminated constituent provided services to the system.

Involuntary Termination:

Involuntary termination may include discharge from service for cause or without cause. Discharge for cause can result from breach of contract, being found guilty of fraud or other criminal behavior, bad dealing, discriminatory behavior or harassment, unlawful or immoral behavior in the work environment, willful neglect of responsibilities, intentionally destroying assets, continuously disregarding organizational policies, and others. If involuntary termination occurs, the terminated constituent's project team leader (PTL) shall notify the designated responsible officer in writing and will identify the conditions under which the constituent's termination occurred. If required, the responsible officer or their designee as may be appropriate shall file any notices required and will comply with all regulatory requirements applicable to the engagement agreement under which the terminated constituent provided services to the system.

Software Development Life Cycle (SDLC) Policy and Procedures:

SDLC Policy Statement:

The Software Development Lifecycle Model describes phases of the software cycle and the order in which those phases are executed to produce deliverables at each phase that are necessary for the next phase in the life cycle to occur. Project requirements are translated into software design characteristics, software design requirements are reduced to code which is referred to as the development phase. Following the coding and development phase, the testing phase verifies the deliverable against the requirements of the design.

The DAC-FICRAS Service System responsible officer for oversight of SDLC policy is:
Michael A. Chester, CDbE, CAE, DAC-FICRAS Chief Technical Officer
Email: support@ficras.com

It is DAC-FICRAS Service System policy to observe and employ the SDLC model when developing new or adapting existing solutions applied within the system. Development phasing of the end system deliverables, whether required in system operations or resulting from specific client request shall consider and be adapted to the following phasing course.

1) **Phase 1 – Identify the current problem or needs** – The process includes gathering input from all stakeholders, including clients, client service associates, sales and marketing associates, industry experts, and others to learn the strengths and weaknesses of the proposed software development and to identify coordination with existing systems where appropriate with enhancement of service control security and delivery of enhanced services as the principal goal.
2) **Phase 2 – Planning –** The identification of software requirements, determines the cost and resources required to develop and deploy the software. It also identifies risks and provides sub-planning options to minimize those risks. In this phase, a software requirement specification (project workbook) document is created.
3) **Phase 3 – Design** – This phase brings the identification and planning phases into a design specification stage where all stakeholders provide review and feedback. A plan of communication is established to provide multi-directional discussion and decision relationships among stakeholders as the project may require.
4) **Phase 4 – Build** – This phase involves development of the code required to perform the services identified and to construct the necessary interfaces that will be required for the software to function as it was designed.

POLICY AND PROCEDURES: (Continued)

SDLC Policy Statement: (Continued)

5) **Phase 5 – Test** – This phase determines whether the software as built performs the desired functions set out in the design construct. The test phase should be made available to stakeholders for testing and input to ensure that modifications made meet the design requirements established for the software.
6) **Phase 6 – Deploy** – Once testing is complete, the software is deployed for either limited or general use by stakeholders in their operations. Deployment can be made to either a specific group of stakeholders or the entire group of users as may be determined to be appropriate. Following deployment, feedback from users is used to assist in identifying modifications that may be required to bring the software deployed to maximum efficiency.
7) **Phase 7 – Maintain** – Following deployment of the software, on-going support, maintenance and monitoring of its use becomes paramount to ensuring maximum productivity. Additional modifications may be identified that improve the software performance. This phase is an ongoing process throughout the software lifecycle.

The goal in utilizing the SDLC model is to provide the smoothest possible flow of ideas and information between the development and operations teams, in a process that delivers high-quality software solutions to all stakeholders within a minimum time period, while also minimizing resource requirements.

SDLC Procedures:

Following identification of new, additional or modified software services that would provide desirable results for DAC-FICRAS Service System users, the constituent identifying the software needs shall contact the responsible officer and provide an overview of the software needs identified.

Within three (3) days of notification of the need identified, the responsible officer or designee as may be the case will determine if the service needs are consistent with those required by DAC-FICRAS Service System clients in general or if there is a reasonable probability the identified software needs will enhance the DAC-FICRAS Service System capabilities for only a single or small group of client(s). Once this determination is completed, the responsible officer will notify the DAC-FICRAS Services Administrator and will provide an overview the findings, to include a technology storyboard and general outline of the responsible officer's vision of the project. The DAC Services Administrator will then assist the responsible officer in identifying stakeholder participants that would work through the SDLC phasing processes. Those constituents identified would form the SDLC Project Team (PT) for that project. The planning phase would begin at this point and the responsible officer would prepare a needs analysis which would include: 1) An overview of the software project, including service probable enhancements to existing systems; 2) an overview of the project service component requirements (communications, accounting, support, etc.) and 3) the relevant costs, potential revenues and risks associated with the project. At this point, a project workbook would be prepared to include the needs analysis report, a storyboard of the software development's SDLC phasing components, a list of stakeholder participants, and the secure communication services that would be available to constituents. Additionally, an accounting and operations support plan and budget to include all project cost accounting would be prepared for inclusion with the project workbook.

The PT leader will immediately request a project communication system to be established for the project, identifying the prospective needs to the responsible officer. The requirements will be reviewed with the DAC-FICRAS Services Administrator and the responsible officer will provide estimates of time and fees required to complete the project being considered, including any project communication or administrative service costs that may be required.

This will then be presented to the DAC Governance Executive Committee Chair for review and approval. Once approved, the project will proceed post-haste through the various phases of the SDLC to deployment, maintenance and monitoring. The project workbook will remain in active status until adequate maintenance and monitoring time has passed allowing complete review and modification of system components as the opportunities present themselves.

Upon project completion, the responsible officer will sign the project workbook once completed and will provide the original to the DAC-FICRAS Services Administrator who will then review the project workbook. Next, the original project workbook will be provided to the DAC Executive Committee for archiving and future use if warranted. All project information, whether it is communications or other components of development are to be held in strictest confidence. The responsible officer shall monitor security and confidentiality at each stage of the SDLC project development.

POLICY AND PROCEDURES: (Continued)

Risk Management Policy and Procedures:

Risk Management Policy Statement:

It is DAC-FICRAS Service System policy to establish and maintain a business impact analysis (BIA) to help identify the most critical business processes and describe the effect of a potential disruption of those processes. Another step in disaster recovery planning is to perform a risk assessment, focusing on the internal and external situations that could negatively affect critical business processes. By understanding the risks associated with business operations, those risks can be better managed and, in some cases, averted if planned for. The responsible officer for risk management policy functions is:

> Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
> Email: administration@ficras.com

Risk Management Procedures:

The risk management responsible officer will call upon internal and external stakeholders to participate in the initial business impact analysis (BIA). The purpose of this analysis is to identify critical business processes and describe its effect of a potential disruption of those processes. The analysis will describe critical assets, both internal and external that could potentially disrupt the function of those assets. This analysis will include the DAC-FICRAS Service System technology infrastructure, operating systems, service providers, developers, technical, administrative and any other functions or personnel that could potentially impact the business of the DAC-FICRAS Service System or the clients it serves. The next step will be to conduct a risk assessment to identify the internal and external situations that could potentially impact the critical processes. The responsible officer shall combine the BIA and risk assessment into a risk management project workbook (RMPW), which will also include a disaster recovery plan for each potential critical business process identified as a potential risk. The format may be generally similar to the following:

Threat	Probability (P) Assign 0.0 through 1.0 value	Impact (I) Assign 0.0 through 1.0 value	Risk = P x I	Risk Ranking low, med, high	Mitigation Measures in place:	Residual Risk Low, Med, High	Comments

Source: http://searchdisasterrecovery.techtarget.com/Risk-assessments-in-disaster-recovery-planning-A-free-IT-risk-assessment-template-and-guide#q5

The responsible officer shall initially prepare the RMPW to include all risk parameters. A copy of the appropriate BIA format will be prepared, together with the risk assessment format for consideration by the risk management team (RMT). RMT participants shall be selected from internal DAC-FICRAS Service System officers and consulting personnel as well as external client personnel to provide input in identifying operational, financial and administrative risks. Any risks identified and analyzed will then be assigned a priority (high, medium, low) status. Those risks identified as high will receive immediate attention in assessment of disaster recovery procedures to be employed to mitigate or perhaps avert that potential risk.

The responsible officer shall call together the initial RMT participants no later than August 1st of each calendar year and will work with the RMT to produce an effective risk management procedure for the initial and future years. The BIA, risk assessment and disaster recovery plan RMPW shall be completed and certified by the responsible officer on or before November 1st of each calendar year. Upon completion, the RMPW will be provided to the DAC Governance Committee and the risks and appropriate mitigation procedures will be identified and monitored in each succeeding year. The RMPW will create an audit trail of the risk management and mitigation processes undertaken in each succeeding year and will provide the framework for on-going risk management for DAC-FICRAS Service System Operations.

POLICY AND PROCEDURES: (Continued)

Continuity Plan Policy and Procedures:

Continuity Plan Policy Statement:

It is the policy of the DAC-FICRAS Service System to establish a policy and procedures statement continuity plan that will provide for annual review of the policy and procedures statement, with updates as needed to ensure the policy and procedures statement is consistent with changing conditions and that all stakeholders are made aware of modifications required to address those changing conditions. In this regard, the policy and procedures statement shall be reviewed on a monthly basis to address any modification requirements as they become known. The responsible officer for this function is:

Gregory G. Johnson, MAI, SR/WA, DAC-FICRAS Services Administrator
Email: administration@ficras.com

Continuity Plan Procedures:

During the 1st ten days of each quarter, the responsible officer shall review the current policy and procedures statement to determine if any of its components require modification to meet changing conditions. Any changes will be noted as additions to the existing policy and procedures statement in effect at that time and will be catalogued as an addendum of changes to the policy and procedures statement for that month, if any.

If needed changes are identified, the responsible officer shall make note of them and identify all stakeholders that could potentially be affected by the changes. Proposed changes shall be communicated to the affected stakeholders for their input.

If the change is identified as critical, the responsible officer shall have the authority to enact temporary policy and procedures changes and will notify all affected stakeholders of the temporary policy and procedures changes. Stakeholders shall be provided such time as necessary for them to review the changes and either recommend they be ratified or declared unnecessary. By so doing, the changes will either be permanently enacted if ratified or removed if declared unnecessary to maintaining the integrity of system operations.

Any permanent changes to this policy and procedures statement approved by the DAC Governance Executive Committee shall be noted in the addendum of changes. The minimum information required to be placed in the addendum of changes shall include 1) the change identification source; 2) the policy and procedures affected by the change; 3) the affected stakeholders; 4) the effect of the policy and procedures change on affected stakeholders; and 5) the effective date of the change. Once a permanent change is made to the policy and procedures statement, those components of the policy and procedures so modified shall be noted within the body of the policy and procedures statement, with reference to the information pertaining to the policy and procedures change actions recorded in the addendum of changes.

The addendum of changes by reference becomes a part of this policy and procedures statement. In no event shall a temporary policy and procedures change be continued for more than six (6) months from the date it was enacted. The responsible officer upon enactment of a temporary change shall immediately notify all affected stakeholders of the process adopted to review temporary changes as may be required from time to time and will establish a communications medium through which those stakeholders can provide input regarding any temporary change enacted. The responsible officer will further secure the input of affected DAC-FICRAS Service System technology and administrative support personnel as well as DAC Governance Committee input to determine the need for making the temporary change permanent or discarding it as unnecessary. For all modifications of any kind, the minimum information identified in the preceding paragraph will be presented in the addendum of changes.

At a minimum, the policy and procedures statement will be reviewed annually, on or before August 31st of each year, to record all identified changes during that preceding year. All changes during any year will be subject to final review and approval by the DAC Executive Committee. This policy and procedures statement is a “living document” and it is recognized that it is subject to change as conditions may warrant. It is the intent of the Continuity Plan to ensure the policy and procedure statement is current and reflective of conditions as they may occur from time to time.

Attestation:

This Policy and Procedures Statement has been reviewed and approved by the DAC Executive Committee as required by the DAC Governance Charter for all authoritative documents relevant to DAC-FICRAS Service System operations.

This Policy and Procedures Statement is effective as of July 12, 2018; 12:10 p.m. Eastern U.S. Time Zone and will continue to be in effect until such time as modifications are approved and recorded in the future. All authorized clients, providers and contributors of the DAC-FICRAS Service System agree to conduct their interactions with the system in accordance with this Policy and Procedures Statement.

For the DAC Governance Committee:

By:

DAC FOUNDING MEMBER FICRAS

DAC-FICRAS Services Administrator
Gregory G. Johnson, MAI, SR/WA
Phone: 727-919-1611
Email: administration@ficras.com
DAC Website: www.valuelynk.com
FICRAS Website: www.ficras.com

ADDENDUM OF CHANGES:

March 29, 2019:	Clerical error change “of a” to “a” History section, Page 3.
May 22, 2019:	Added record of Personnel New Hire background search requirement, Page 21
Nov. 19, 2019	Updated headings to coincide with body components of P&P statement and procedures
Jan. 6, 2020	Page 10 - **General Use and Ownership of Information** section 2nd sentence in paragraph – change ***or*** for ***and*** as follows: Each constituent having access to said proprietary information must ensure through legal ***and*** technical means that proprietary information is protected in accordance with the Acceptable Use Policy Statement, including the following:
April 13, 2021	Modification of Change Management Procedures: Added Cheryl Bella, MAI, AI-GRS as team lead for FICRAS change management and removed the DAC Executive Committee approval requirement. This was the result of meeting with DAC Executive Committee Chairman, Lawrence J. Golicz, PhD., MAI, ASA – deemed a redundant approval clause that should be removed.
June 1, 2021	Pagination modifications only
September 1, 2021	Policy and Procedures review – no changes required
March 31, 2022	Policy and Procedures review – no changes required
July 31, 2022	Policy and Procedures review – no changes required
September 22, 2022	Policy and Procedures review – table of contents pagination change – Continuity Plan and Procedures from Page 26 to Page 27
January 25, 2023	Policy and Procedures review – No modifications required.
April 30, 2023	Policy and Procedures review – No modifications required.
May 15, 2023	Policy and Procedures review – Considering modification to address ESG issues as they come Into being. There is strong indication that ESG analysis of the DAC-FICRAS system may be required in the next 12 months. Continuing inquiry regarding this issue and will report in next P&P review.
November 15, 2023	Policy and Procedures review – ESG services are continuing to be considered. No requests for these services are noted from operations; however, at least one of our support staff has been obtained training and certification regarding ESG reporting since the last review. We will continue monitoring P&P requirements and will make adjustments as required for this and other services the DAC is likely to offer to its clients and other subscribers.
April 1, 2024	Policy and Procedures review – ESG services monitoring continuing. Various 3rd party service provider integrations, Abrigo LOS, ValNow AVM, Servicelink Flood Mapping, Verisk Replacement Cost Estimating, are being readied for deployment. These will be monitored for any issues that would require modification of this policy and procedures statement.