U.S. General Services Administration
Federal Advisory Committee Act Database (FACA DB)

Rules of Behavior

Version 1.0

July 25, 2018

Table of Contents

1 Introduction

The Federal Advisory Committee Act Database (FACA DB) Rules of Behavior (RoB) are designed to ensure that all authorized users of FACA DB resources are aware of their responsibilities and expected behavior in safeguarding those resources. FACA DB resources include anything associated with the FACA DB information system.

1.1 Applicability

The FACA DB RoB applies to all FACA DB authorized users with access rights via assigned user IDs and passwords. FACA DB users are Federal Government employees or authorized contractors. The FACA DB RoB for the utilization of FACA DB are consistent with each user's employing agency's RoB for the use of any public facing, open, and transparent Federal Government system.

1.2 References

The following documents provide additional information regarding the determination of the security categorization of a system:

- Appendix III, Office of Management and Budget (OMB) Circular A-130 – Security of Federal Automated Information Resources;
- Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541;
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: the NIST Handbook;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- GSA Order CIO P 2100.1, GSA IT Security Policy;
- GSA Order CIO 2160.2, GSA Electronic Messaging and Related Services;
- GSA Order CPO 1878.1, GSA Privacy Act Program;
- GSA Order CIO 2100.3, Mandatory IT Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities;
- GSA Order OGC 7800.11A ADM, Personal Use of Agency Office Equipment;
- GSA Order CIO 2106.1, GSA Social Media Policy;
- GSA Instructional Letter, IL-12-01, Mobile Device Applications;
- GSA Order CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

1.3 Information System Description

The FACA DB is a cloud-based system residing on a Salesforce platform. The FACA DB is used by Federal agencies to continuously create, operate, manage, and terminate an average of 1,000 advisory committees government-wide. In addition, the FACA DB is used by Congress and the General Accounting Office to perform oversight of related Executive Branch programs and by the public, the media, and others, to stay abreast of important developments resulting from advisory committee activities.

Although centrally supported by the GSA's Committee Management Secretariat (CMS), the FACA DB represents a true "shared system" wherein each participating agency and individual committee manager has responsibility for providing accurate and timely information that may be used to assure that the system's wide array of users has access to the data required to be collected by FACA. The FACA DB provides all agencies with advisory committees the ability to report and update activities as required by law, and this information is available to the public.

1.4 Roles and Responsibilities

The FACA DB System Owner must, for the Secretariat staff, and through executive branch Committee Management Officers (CMOs):

- Ensure that authorized users, including Federal Government employees and contractors, who access FACA DB resources, acknowledge they will comply with the RoB.
- Coordinate and arrange system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization)

Authorized users must use FACA DB resources in an ethical and lawful manner and comply with the FACA DB RoB and the federal policies referenced in this order.

1.5 Penalties for Non-Compliance

Users who do not comply with the RoB may incur disciplinary action, as well as civil and criminal liability.

2 FACA DB Rules of Behavior

Category	Rules of Behavior
Personal Use	GSA provides the FACA DB system resources for official use and FACA DB authorized users must not use IT resources for their own or others private gain, commercial purposes (including endorsement), or profit-making activities.
User Accounts	Committee Management Officers (CMOs) manage access to the FACA DB only for their agency/department. CMOs request the addition of user accounts for their agency/department, and account access is only for individuals who have a business need for entering, modifying, or reviewing data in the FACA DB. CMOs annually will review and certify the list of users at their agency/department that have a business need for a FACA DB user account. In addition, CMOs will request inactivation of users during the year if/when they no longer require access (e.g., if they retire or no longer have FACA duties). When adding/removing users/committees from Groups, CMO's must ensure they make the correct assignments. Users are authorized to have access only to committees and groups to which they have been officially assigned by their agency/department. If users discover they have access to FACA database committees to which they have not been assigned, they should promptly report the error as follows: DFO and GFO users are to report errors in access rights to their CMO, and CMOs are to report errors in access rights to their CMS Desk Officer. CMS staff will require appointment documentation from each agency/department before CMO user access is granted.
Privacy	FACA DB users have no expectation of privacy on GSA IT resources since all activities are subject to monitoring. Take measures to protect Personally Identifiable Information (PII) and sensitive data and do not post such data to the FACA DB.
Protection	Protect FACA DB resources from theft, destruction, or misuse.

Access	Users must access the FACA DB only through authorized interfaces. Maintain the confidentiality of passwords; do not share passwords with anyone, including other employees, management, or technical personnel; and do not write, display, or store passwords where others may access or view them. Do not attempt unauthorized access to any part of the FACA DB system. Logoff the FACA DB system once work has been completed or the authorized workstation will be left unattended.
Antivirus Protection	Do not interfere with GSA-provided antivirus protection on GSA IT resources and provide and maintain up-to-date antivirus protection software on personally owned resources that access to FACA DB.
Prohibited Usage	Never convey any material that is sexually explicit, offensive, abusive, discriminatory or objectionable or browse sexually explicit or hate-based web sites through the FACA DB. Never transmit non-business related large attachments, chain letters, unauthorized mass mailings, or intentionally send malware through the FACA DB. Never use copyrighted or otherwise legally protected material without permission when posting to the FACA DB. Never use FACA DB resources to "snoop" on or invade another person's privacy or break into any computer, whether belonging to another organization. Never transmit any material that is libelous or defamatory on the FACA DB.
Reporting	Promptly report, to the FACA DB System Owner and FACA DB Information Systems Security Officer (ISSO) any observed or suspected security problems/ incidents, including loss/theft of IT resources, or persons requesting that you reveal your password.

3 Acknowledgement

The above sections presented general guidelines for protecting the FACA DB system and associated information. These rules are a great reference for stating what you, as a user, should and shouldn't do when accessing or using the FACA DB system. Please acknowledge that you've read and understood the FACA DB RoB as written above. Acknowledgement of the FACA DB RoB is a requirement to receive initial or continued access to the FACA DB information system.

I hereby acknowledge that I have read and agree to the FACA DB Rules of Behavior.

_____
Signature

_____
Printed Name

_____
Date

User Account Role in FACA DB (Select One):
_____CMS Staff
_____CMO Account User
_____GFO/DFO Account User