

SYSTEM NAME AND NUMBER:

Information Technology Service Ticket System–FTC (FTC-VII-7).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

System data are currently maintained off-site by an FTC contractor.

For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC’s website at <https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 80 FR 9460, 9465 (Feb. 23, 2015).

SYSTEM MANAGER(S):

Core Engineering and ISSO Services Program Manager, Office of the Chief Information Officer, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, email: SORNs@ftc.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 et seq.

PURPOSE(S) OF THE SYSTEM:

To register, track and control usage of office telephones, cell telephones and other telecommunication devices by individual users; to record the receipt of requests for information technology (IT) service by the FTC’s enterprise service desk (i.e., help desk) and the actions taken to resolve those requests; to provide agency management with information identifying trends in questions and problems for use in managing the Commission’s hardware and software

resources. The FTC's help desk, currently operated by a contractor, generates and maintains these records ("service tickets") in the course of fulfilling requests or orders to create or close e-mail and other network accounts when an individual begins or ends employment at the FTC, to answer questions or provide assistance when FTC staff have problems with computer or network access or other FTC IT equipment or software issues, etc.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

FTC employees, contractors or other authorized individuals who have requested service related to the automated information technology equipment and systems available to the FTC staff (e.g., computers, laptops, etc.).

CATEGORIES OF RECORDS IN THE SYSTEM:

FTC personnel, consultants, and contractors assigned office telephones, cell phones, or other telecommunications resources; name of requesting individual, organization code, telephone number, date of reported problem, nature of problem, and action taken to resolve problem.

RECORD SOURCE CATEGORIES:

Individual about whom the record is maintained and staff who responded to the request for service.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system may be compiled and used by the FTC's contractors to track and fulfill IT service requests. For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at

<https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 83 FR 55542-55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Data are entered and stored in the system electronically by the FTC's help desk contractor using proprietary software in a structured database.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by employee name and tracking number assigned to each service request.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained according to GRS 5.8 and are destroyed 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access is restricted to agency personnel and contractors whose responsibilities require access. Electronic access to FTC records in the contractor's database is provided via the Internet, using unique IDs and password combinations, and can be accessed only from Internet Protocol (IP) addresses belonging to the FTC. When not in use, access automatically "times out" (cuts off) after 30 minutes. The contractor's servers have firewalls and intrusion detection, and are maintained in locked rooms secured with electronic card access.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at <https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at <https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at <https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems> and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

80 FR 9460-9465 (February 23, 2015)

73 FR 33591-33634 (June 12, 2008).