Operational Policy

Policy title:	Geographic Bounds of Data Access Policy		
Policy number:	ODHS|OHA 090-018		
Original date:	09/12/2022	**Last update:**	09/12/2022
Approved:	Kris Kautz, Deputy Director OHA Don Erickson, Chief Administrative Officer ODHS		

Purpose

The Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) are committed to protecting information assets and systems from unauthorized access, modification, destruction, and disclosure. The purpose of this policy is to prohibit access to agency data from outside of the United States (U.S.) including U.S. territories unless approved.

Description

This policy describes the requirements for approval and the necessary safeguards for remote access to ODHS|OHA information from outside the U.S.

Applicability

This policy applies to all ODHS|OHA staff including employees, volunteers, trainees, and interns as well as partners and contractors.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Policy

1. ODHS|OHA staff shall not access agency data from outside of the U.S.
2. ODHS|OHA staff who require access to agency data from outside of the U.S. for a business need, shall request an exception by completing the MSC 3483 Geofencing

Exception Request Form. (Refer to ODHS|OHA 090-009-05 Geofencing Exception Request Process)

3. When access is requested on behalf of a third-party entity, ODHS|OHA staff shall follow the ODHS|OHA 090-009-05 Geofencing Exception Request Process.
4. All exception requests to work from outside the U.S. shall be reviewed by the Information Security and Privacy Office (ISPO) and approved in writing by individual staff's manager, agency leadership and the information system owner, who is the person accountable for the information created, transmitted, received, and processed by the specific system.
5. If the request for remote work is approved, the Chief Information Risk Officer (CIRO) shall contact the Enterprise Information Services (EIS) Cyber Security Services (CSS) to implement the requested exception.
6. ODHS|OHA staff, partners, and contractors who are approved for remote access from outside of the U.S., shall be responsible for following applicable state and federal requirements for access and protection of confidential data.

References

45 CFR 164.302-164.318 Security Standards for the Protection of Electronic Protected Health Information

Criminal Justice Information Systems Security Standards (CJIS)

Department of Defense Policies, Procedures, and Practices for Information Security Management of Covered Systems, Report No. DODIG-2016-123

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume I Harmonized Security and Privacy Framework Version 2.2

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Rev. 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

Center for Internet Security Controls

ODHS|OHA 090-090-009-05 Geofencing Exception Request Process
ODHS|OHA 090-014 Password Policy
ODHS 010-023-02 Working Remote-Within the state of Oregon
ODHS 010-023-03 Working Remotely: Confidentiality and Security
ODHS 010-023-04 Working Remotely Out of State
ODHS 010-023-09 working Remotely Working Out of State
ODHS|OHA 070-001 Mobile Communication Device Policy
U.S. Department of the Treasury, Office of Foreign Assets Control-Sanctions Programs, and Information
OWL Office of Information Services Single Device Project FAQ VPN FAQ

Forms
MSC 3483 Geofencing Exception Request Form

Related policies
DAS 50.050.01 Working Remotely
DAS 107-004-110 Acceptable Use of State Information Assets
ODHS|OHA 090-003 Access Control Policy
OHA 010-023 Flexible Work Solutions

Contact
Information Security and Privacy Office (ISPO)
Phone: 503-945-6812; dhsinfo.security@odhsoha.state.or.us

This policy shall be reviewed at least once every year to ensure relevancy.

Policy history
Version 1 ODHS 090-018 established 09/12/2022

Keywords
Access, geofencing, geographic, remote, U.S., U.S. territories

---