

WORKING REMOTELY | WORKING OUT OF STATE



Topics for Consideration

Employees may bring forth the idea of working remotely on a full- or part-time basis. When considering the approval of remote work that would take place outside of Oregon, there are many different workplace topics to consider in making this business decision.

This document is not intended as a checklist for approving out of state remote work. It is to highlight potential distinctions in managing employees who are working out of state.

HUMAN RESOURCES

Background Checks

Consult with DOJ – background check requirements or limitations may vary by state.

I-9 Compliance

For those working out of state at the time of hire, a representative will need to be found to physically examine the I-9 documents and complete on the agency's behalf.

Consult with DOJ - some states have enacted laws regarding immigration employment eligibility verification.

Pay Equity

The safest practice is to apply Oregon's pay equity law when determining compensation or making adjustments to salary. (Oregon's law is among the most comprehensive.) In most cases, this will be most beneficial to the employee and, for Oregon, will maintain internal equity.

Civil Rights

Consult with DOJ - some states may have protected classes beyond those protected by Oregon or Federal law.

Paid/Unpaid Leave Entitlements

Consult with DOJ - requirements to provide paid or unpaid leave may vary by state.

Protected Leave Entitlements

Consult with DOJ - protected leave entitlements or requirement to pay while on protected leave may vary by state.

ADA Accommodations

Employers have the obligation to accommodate employees, including those who are working remotely out of state, absent undue hardship.

Bargaining

If any provisions within a remote work agreement for a represented employee depart from DAS policy or CBA, discuss the agreement with labor prior to execution.

PAYROLL AND BENEFITS

Wage and Hour Laws

Consult with DOJ - wage and hour laws, such as minimum wage, overtime and paydays vary by state.

PEBB Coverage

The following PEBB benefits are nationwide:

- Providence statewide plan - in-network coverage
- VSP and Delta Dental
- Standard Insurance
- Flexible spending accounts
- Long term disability
- Employee Assistance Program (EAP)

Unemployment Insurance

Consult with DOJ - withholding requirements vary by state.

Tax Withholdings

The employee is responsible for calculating and paying their individual tax liabilities. Agencies cannot advise whether employees may have tax obligations in another state and cannot advise employees on their Oregon tax liability. If the employee provides an Oregon W-4, we may rely upon that for Oregon withholding purposes. If no Oregon W-4 is completed, withholdings will be calculated at the Single with no exemptions rate.

SAFETY AND RISK

Workers Compensation

Contact DAS Risk for determination of workers compensation coverage.

The Oregon tort cap does not apply to lawsuits filed in different states.

OSHA Considerations

States covered by Federal OSHA - Federal OSHA applies

States covered by their own OSHA plans – unknown which state plan would apply

The employer is only responsible for violations about which it could have reasonable known. The risk of enforcement action or other OSHA intervention is very low when the employee is working from their home.

TRAVEL TIME AND REIMBURSEMENT FOR TRAVEL EXPENSES

Follow the Fair Labor Standards Act (FLSA).

Consult with DOJ to determine if other state's laws are more generous than the FLSA.

Follow the Oregon Accounting Manual for state travel reimbursement practices.

INFORMATION SECURITY

Location

Consult with DOJ - The Department of Treasury maintains a list of countries that present a threat to national security, <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>. Remote access from these countries is highly discouraged and agencies are encouraged to seek legal advice before permitting.

Identity and Access Management

Multi – Factor Authentication (MFA) is required to access the State network. The second authentication must be an approved authenticator app on a separate state owned device or other method that meets the requirements of statewide standard.

Privileged access accounts are not permitted to access resources from outside the US.

Approval of employees working outside of the US must be kept documented and kept on file.

Device Management

Employees must use only state issued devices, no personal devices allowed.

Devices need to be under agency device management and meet all statewide standards. Agencies must validate their device management operates and functions as designed in the remote country.

Encryption Requirements

Encryption must meet or exceed the State Security Standards, in particular:

- All storage devices (laptop, workstation phone drives, removable storage devices) must be encrypted at rest using FIPS-140-2 compliant encryption.
- Encryption ciphers must be FIPS-140-2 compliant (ex: AES 256) as stated in the State Security Standards.
- No sharing of the encryption keys (VPN, workstation, mobile device, etc.)
- Web Traffic must be encrypted using TLS 1.3 or 1.2

Network Requirements

State devices connecting to the state network must connect using Virtual Private Network (VPN)

No data roaming on state owned devices.

Created in partnership between Enterprise Information Services, DAS Risk Management, DAS Financial Business Systems, DAS Statewide Accounting and Reporting Services, the Chief Human Resources Office and the Department of Justice.