This document is for educational purposes only and needs to be customized further. Reach out to the State Privacy Officer at wphillips@utah.gov before implementation.

Bring Your Own Device Policy Template

(this document is related to the Privacy Program requirement under The Utah Government Data Privacy Act)

Purpose:
The purpose of the Bring Your Own Device (BYOD) policy is to allow employees to use their personal devices for work-related activities, enhancing flexibility and productivity, while ensuring that our organization's data and information remain secure.

Scope:
This policy applies to all employees who choose to use their personal laptops, smartphones, or tablets for work-related activities.

Policy Guidelines:

1. **Eligibility and Approval:**
    - Employees must receive written approval from their department heads to use personal devices for defined work purposes.
    - Only devices meeting the IT department's security and compatibility standards will be allowed.
    - Devices must undergo a security and compatibility assessment before approval.

2. **Security Requirements:**
    - Devices must be equipped with up-to-date antivirus software and a secure lock screen.
    - Devices must be updated to the latest operating system version supported by the manufacturer and approved for work purpose.
    - The IT department must install necessary work-related software and configurations, including VPN, encryption tools, and remote wipe capabilities.
    - Multi-factor authentication (MFA) must be enabled on all personal devices used for work.

3. **Mobile Device Management (MDM):**
    - All personal devices used for work must be registered with the company's MDM system.
    - MDM software will manage the configuration and security of work-related settings and applications.
    - MDM will enable the IT department to remotely wipe company data from the device if it is lost, stolen, or if the employee leaves the company.
    - Employees must agree to the installation of MDM software and regular security updates.

4. **Data Management:**
    - Sensitive or otherwise highly classified data should not be stored locally on personal devices whenever possible.
    - Employees are responsible for backing up personal data. [Company Name] is not responsible for the loss or recovery of personal data on employee devices.

5. **Compliance and Monitoring:**
    - Devices may be subject to periodic audits and compliance checks by the IT department.
    - Devices may be subject to open records requests (GRAMA) or legal discovery actions.
    - Any device that is lost or stolen must be reported to the IT department immediately.
    - Employees must comply with all relevant federal, state, and local regulations regarding data security and privacy.

6. **Acceptable Use:**
    - Personal devices used for work must not be used by anyone other than the authorized employee.
    - Employees must comply with all existing policies regarding the use of technology and the handling of confidential information.

- Work-related activities on personal devices must adhere to the organization's acceptable use policy.

7. **Termination of Access:**
    - Access to company resources from personal devices can be revoked at any time without prior notice for security reasons.
    - Upon termination of employment, employees must immediately cease using personal devices for work-related purposes and ensure that all company data is completely removed from their devices.
    - Employees must return any organization-provided accessories or peripherals upon termination.

8. **Help and Support**
    - Personal devices and software not utilized for approved work purposes are not eligible to receive support from the governmental agencies' information technology organization.
    - The employee's organization will not be held liable for any damage that may occur to personal devices used for work purposes. Employees should have no expectation of repair or replacement for their personal devices. Use of personal devices for work is entirely at the employee's own risk.
    - Support for work-provided software and applications will be provided through the IT helpdesk.

9. **Cost Reimbursement:**
    - The organization will / will not reimburse employees for the cost of personal devices or their maintenance, repair, or replacement.
    - The organization may reimburse employees for work-related mobile data usage if pre-approved by the department head.

10. **Privacy Considerations:**
    - The organization reserves the right to access, monitor, and review all data and communications on personal devices used for work purposes, in accordance with applicable laws and regulations.
    - Personal data will not be accessed or monitored by the organization unless required by law.

Acceptance: Employees must sign an agreement acknowledging that they have read, understood, and agree to abide by the BYOD policy, including the management of their devices through the MDM system.