CORRECCIONAL JUVENIL DE OREGON

Declaración de la política

Parte I: servicios administrativos

Asunto:

Dispositivos móviles de comunicación (celulares) y otros dispositivos móviles de almacenamiento de datos

Sección – Número de política:	*Sustituye a:*	*Fecha de entrada en vigencia:*	*Fecha de la última actualización /revisión:*
C: gestión de la propiedad – 9.0	**I-C-9.0 (10/21)** **I-C-9.0 (12/18)** **I-C-9.0 (06/13)** **I-C-9.0 (06/10)** **I-C-9.0 (09/08)** **I-C-9.0 (06/03)** **I-C-9.0 (02/99)**		**Ninguna**

Normas y referencias relacionadas:	▪ División de Gestión de Recursos de Información (Information Resources Management Division (IRMD, por sus siglas en inglés)) del Departamento de Servicios Administrativos (Department of Administrative Services (DAS, por sus siglas en inglés)); (DAS-IRMD), Políticas informáticas del estado de Oregon ▪ Política y estrategia de información empresarial del Departamento de Servicios Administrativos: ▪ 107-001-0015 (Controles internos para la gestión de los dispositivos móviles de comunicación) 107-004-051 (Control de dispositivos de almacenamiento portátiles y extraíbles) 107-009-0050 (Adquisición y eliminación sostenible de equipos electrónicos) 107-001-016(Uso de dispositivo móvil de comunicación al conducir) 107-004-100 (Transporte de activos de información) ▪ Dirección de Recursos Humanos del Departamento de Servicios Administrativos: 50-050-01 (Trabajo remoto) ▪ Política de la Correccional Juvenil de Oregon (Oregon Youth Authority (OYA, por sus siglas en inglés)): 0-7.0 (Uso de activos y sistemas electrónicos) I-C-2.0 (Uso de vehículos de propiedad estatal) I-C-1.0 (Sistemas de control de la propiedad) I-E-1.4 (Gestión de registros públicos) I-E-2.0 (Conservación, destrucción y archivo de registros) I-E-2.3 (Solicitudes de información y registros de los jóvenes) I-E-3.2 (Clasificación y protección de activos de información) I-E-3.3 (Respuesta a incidentes de seguridad de la información) II-A-1.0 (Acceso a los centros) II-A-3.1 (Transporte de los jóvenes)
Procedimientos relacionados:	▪ Ninguno

Responsable de la política: Director de información	**Aprobada por:** _____ Joseph O'Leary, director

I. PROPÓSITO:

Esta política describe las normas para el personal de la OYA en relación con la protección de la información de la OYA que está almacenada en dispositivos móviles de almacenamiento de datos y la gestión de los dispositivos móviles de comunicación de propiedad estatal.

II. DEFINICIONES DE LA POLÍTICA:

Información crítica: información que se considera extremadamente sensible y que está destinada a ser utilizada únicamente por una o varias personas designadas. Esta información suele estar exenta de la divulgación pública porque, entre otras razones, dicha divulgación podría causar posiblemente daños o perjuicios importantes, incluso la muerte, a la(s) persona(s) designada(s), a los empleados, clientes o socios de la agencia o causar un daño importante a la agencia.

Información limitada: información sensible que puede no estar protegida de la divulgación pública, pero que si se pone a la disposición del público de forma fácil e inmediata, puede poner en peligro la privacidad o la seguridad de los empleados, clientes o socios de la agencia. La OYA debe seguir sus políticas de divulgación antes de proporcionar esta información a personas externas.

Dispositivo móvil de comunicación (Mobile Communication Device (MCD, por sus siglas en inglés)): es un dispositivo de mensajes de texto o de comunicación inalámbrica bidireccional (celular) que está diseñado para recibir y transmitir mensajes de voz o de texto, incluyendo los Sistemas de Posicionamiento Global (Global Positioning Systems (GPS, por sus siglas en inglés)) móviles, y los teléfonos y relojes inteligentes.

Dispositivo móvil de almacenamiento de datos: un dispositivo electrónico que almacena datos y está diseñado para la portabilidad (por ejemplo, un dispositivo móvil de comunicación, una computadora portátil, una unidad de memoria flash USB, un CD, un DVD, una tableta, un dispositivo para videojuegos, un MCD).

Información restringida: información restringida destinada al uso laboral limitado que puede estar exento de la divulgación pública porque, entre otras razones, dicha divulgación pondría en peligro la privacidad o la seguridad de los empleados, clientes, socios de la agencia o las personas que, de otro modo, califican para una exención. Solo se puede acceder y utilizar la información de esta categoría por personas internas cuando estén específicamente autorizadas a hacerlo en el desempeño de sus funciones. Las personas externas que soliciten esta información para asuntos autorizados de la agencia deben adquirir una obligación contractual de confidencialidad con la agencia antes de recibirla.

III. POLÍTICA:

La OYA ha identificado a la diversidad, equidad e inclusión (Diversity, Equity, and Inclusion (DEI, por sus siglas en inglés)) como una prioridad e iniciativa de la agencia; con el objetivo de construir un entorno respetuoso, diverso, equitativo e inclusivo para los jóvenes y el personal, el cual está libre de acoso, discriminación y prejuicios. La disponibilidad y el uso de los dispositivos móviles de comunicación de propiedad estatal deben apoyar esta iniciativa.

La OYA controla y protege físicamente los dispositivos móviles de almacenamiento de datos, así como protege y gestiona cualquier información almacenada en ellos. Los controles protegen contra el robo de equipos de propiedad estatal, la divulgación no autorizada de información, el uso incorrecto de los equipos o el acceso no autorizado a la información y los dispositivos.

Por lo general, la información de la OYA se almacenará en la red de la OYA. El personal puede cargar la información de la OYA en los dispositivos móviles de almacenamiento de datos de propiedad estatal para realizar su trabajo inmediato. El personal solo puede llevar una cantidad de información necesaria fuera de las instalaciones de la OYA para realizar sus funciones. Consulte la política de la OYA I-E-3.2 (Clasificación y protección de activos de información) en relación con la forma en que deben protegerse los diferentes niveles de sensibilidad de la información.

Los dispositivos móviles de comunicación (MCD, por sus siglas en inglés) de propiedad estatal solo pueden utilizarse para asuntos estatales. Sin embargo, se permite un uso personal limitado y casual siempre que no suponga un costo para el Estado o sea insignificante. Solo aquellos cuyas funciones laborales requieran el uso de un MCD pueden recibir un MCD de propiedad estatal y son usuarios autorizados para los cargos del plan. La OYA solo pagará los cargos del plan de un MCD para los usuarios autorizados.

Los dispositivos móviles de comunicación y los dispositivos móviles de almacenamiento de datos proporcionados por la OYA son propiedad de la agencia. La OYA se reserva el derecho de investigar, recuperar y leer cualquier comunicación o datos compuestos, transmitidos o recibidos a través de los servicios de voz/datos, conexiones en línea o almacenados en sus servidores o propiedad sin previo aviso al personal, en la medida máxima permitida por la ley.

El incumplimiento de cualquier disposición de esta política o las normas contenidas en la misma, puede dar lugar a la adopción de medidas disciplinarias, que puede incluir y llegar hasta el despido del servicio estatal.

IV. NORMAS GENERALES:

A. El personal solo debe utilizar los equipos de propiedad estatal y proporcionados por el Estado (por ejemplo, computadoras, impresoras, celulares, unidades de memoria flash) para llevar a cabo los asuntos estatales. El equipo personal no debe utilizarse para acceder a los sistemas del Estado o para llevar a cabo asuntos estatales.

B. Cuando se conecte un dispositivo móvil de almacenamiento de datos de propiedad estatal a una red inalámbrica, el personal debe conectarse a los recursos disponibles en el siguiente orden:

1. El punto de acceso inalámbrico seguro de la OYA;

2. Utilizar la función “punto de acceso personal” en un dispositivo de la OYA, o un dispositivo con conexión a un punto de acceso de la OYA; o

3. Las redes inalámbricas públicas (por ejemplo, cafeterías, hoteles).

C. Las conversaciones y los mensajes de texto a través de los dispositivos móviles de almacenamiento de datos de propiedad estatal deben limitarse a información no restringida y no crítica siempre que sea posible. Si se discute o escribe información restringida o crítica, el personal debe intentar hacerlo fuera de la vista o del alcance del oído de los demás.

D. El personal debe asegurarse de que el dispositivo móvil de almacenamiento de datos autorizado esté protegido por una contraseña al iniciar la sesión.

E. El personal debe asegurarse de que el dispositivo móvil de almacenamiento de datos autorizado esté cerrado con llave en un cajón, un armario o una habitación cuando no se utilice.

F. El personal debe asegurarse de que el dispositivo móvil de almacenamiento de datos autorizado esté encriptado.

G. El personal debe asegurarse de que los jóvenes no usen o accedan a los MCD o a los dispositivos móviles de almacenamiento de datos del personal, con una excepción. El personal puede permitir que un joven utilice un MCD de propiedad estatal cuando sea necesario para apoyar el plan de caso o los objetivos del joven, y el personal debe supervisar directamente al joven todo el tiempo.

H. La OYA se reserva el derecho de eliminar **toda** la información de un dispositivo móvil de almacenamiento de datos de propiedad estatal si el empleo de un miembro del personal termina con la OYA o si el dispositivo móvil de almacenamiento de datos de propiedad estatal del miembro del personal se pierde, lo roban, no funciona correctamente o lo reemplazan.

1. El personal debe notificar inmediatamente a un supervisor (o al oficial del día) y llamar al servicio de atención al usuario de los Servicios de Información, (503) 378-4333 (opción 2), si el dispositivo se pierde, lo roban, lo reemplazan o ya no se necesita para los asuntos de la OYA.

   Consulte la política de la OYA I-E-3.3 Respuesta a incidentes de seguridad de la información, para obtener instrucciones adicionales si el dispositivo perdido o robado contiene información restringida o crítica.

2. Recursos Humanos debe notificar al servicio de atención al usuario de los Servicios de Información la desvinculación laboral de un miembro del personal de la OYA en o antes de la fecha de desvinculación del personal.

I. La información almacenada en un dispositivo móvil de almacenamiento de datos de propiedad estatal está sujeta a las leyes de registros públicos.

Es posible que la OYA necesite acceder a un dispositivo móvil de almacenamiento de datos de propiedad estatal para obtener datos o información en caso de una investigación personal o penal relativa a un asunto de la OYA.

J. Los MCD de propiedad estatal

1. El personal debe llevar un MCD de propiedad estatal cuando transporte a los jóvenes y cuando realice visitas a los domicilios de los jóvenes.

2. El personal debe utilizar un accesorio de manos libres cuando conduzca un vehículo mientras utiliza un MCD de propiedad estatal.

   a) Se aconseja al personal que emplee precaución extrema cuando utilice un MCD mientras conduce un vehículo, debido a la posibilidad de que se produzcan más accidentes de tráfico mientras se conduce y se utiliza un MCD.

      El método preferido para utilizar un MCD mientras se conduce un vehículo es estacionar el vehículo en un lugar seguro antes de utilizar el MCD.

b) Cualquier infracción de tráfico o el pago de las multas impuestas por la violación de cualquier ley aplicable, incluidas las relativas al uso del MCD, es responsabilidad individual del miembro del personal.

K. El personal no debe almacenar información de la OYA en dispositivos móviles de almacenamiento de datos personales.

L. El personal debe actualizar los sistemas operativos de sus dispositivos en todos los MCD siempre que haya una nueva versión disponible o cuando así se lo indiquen los Servicios Técnicos.

V. ADQUISICIÓN Y CONTROL DE LOS MCD DE PROPIEDAD ESTATAL

A. Se designa a un miembro del personal de los Servicios de Información como coordinador del plan de comunicaciones móviles de la OYA.

1. El coordinador del plan de comunicaciones móviles:

a) Está autorizado para abrir, gestionar y cancelar las cuentas autorizadas de los MCD;

b) Está autorizado para adquirir todos los MCD para la OYA;

c) Sirve de contacto y enlace con el Departamento de Servicios Administrativos (DAS, por sus siglas en inglés) y el distribuidor;

d) Se asegura de la desconexión de los servicios de acceso de los MCD perdidos o robados; y

e) Mantiene una lista de todas las cuentas de acceso a los MCD y de los usuarios correspondientes autorizados (nombres del personal), así como de las cuentas con propósitos especiales.

2. Los supervisores deben solicitar los MCD y los servicios a través del coordinador del plan de comunicaciones móviles mediante la creación de una orden de trabajo de los Servicios de Información (Information Services (IS, por sus siglas en inglés)).

B. Los supervisores deben determinar si un miembro del personal necesita utilizar un MCD de propiedad estatal para realizar sus funciones.

1. Las razones válidas para necesitar un MCD de propiedad estatal incluyen:

a) Las funciones oficiales exigen que el personal esté “en servicio” fuera de las estaciones de trabajo;

b) Las funciones oficiales exigen grandes desplazamientos durante el tiempo normal de trabajo asignado al personal;

c) Las funciones oficiales exponen al personal a peligros fuera del lugar de trabajo; o

d) Las funciones oficiales exigen una respuesta de emergencia o de tiempo crítico.

e) El costo del dispositivo está justificado por el beneficio de eficiencia operativa.

2. El supervisor del lugar de trabajo podrá distribuir los MCD cuando lo considere adecuado.

C. Revisión de la facturación de los MCD de propiedad estatal

Contabilidad debe auditar las facturaciones mensuales para identificar un posible uso inadecuado del MCD y cualquier error de facturación.

D. Uso adecuado de los MCD de propiedad estatal

Cuando el personal es designado como usuario autorizado de un MCD de propiedad estatal, dicho uso está destinado a asuntos relacionados con el Estado. Sin embargo, se permite un uso personal limitado y casual siempre que no suponga un costo para el Estado o sea insignificante.

1. Solamente la OYA puede determinar si el uso por parte del personal es de carácter personal o comercial.

2. Se podrá exigir al personal que reembolse a la OYA el uso personal no autorizado de un MCD de propiedad estatal.

E. Consulte la política de la OYA II-A-1.0 (Acceso a los centros) para conocer las directrices sobre el transporte de los MCD en los centros de la OYA.

F. Los supervisores deben asegurarse de que el personal al que autorizan a utilizar los MCD de propiedad estatal comprenda el uso aceptable de los MCD, y que el personal complete un curso obligatorio de Workday Learning que incluya la revisión de esta política.

VI. CONTROL DE LOS DISPOSITIVOS MÓVILES DE ALMACENAMIENTO DE DATOS DE PROPIEDAD ESTATAL

A. Asignación de dispositivos móviles de almacenamiento de datos de propiedad estatal (distintos de los MCD)

1. La asignación de equipos de propiedad estatal, incluidos los dispositivos móviles de almacenamiento de datos, deben documentarse en Workday mediante la Encuesta de activos, que puede encontrarse escribiendo “Asset survey” [Encuesta de activos] en la barra de búsqueda en la parte superior de la pantalla de Workday. Si necesita ayuda para llenar la encuesta de activos en Workday, consulte el siguiente enlace: TechTip – “Workday Asset Survey response guide” [Consejo técnico: guía de respuestas de la encuesta de activos de Worday].

2. El personal debe llenar una nueva encuesta de activos de Workday cuando su equipo asignado cambie.

B. Transporte de los dispositivos móviles de almacenamiento de datos de propiedad estatal

1. El personal debe tener autorización para retirar el dispositivo de almacenamiento del lugar de trabajo. La autorización depende de la asignación de trabajo y del protocolo local.

2. Deben seguirse los protocolos relacionados con el registro de los dispositivos de almacenamiento extraíbles (por ejemplo, firmar por una computadora portátil).

3. Transporte en vehículos

a) El personal debe mantener el control físico del dispositivo móvil de almacenamiento de datos durante todo el transporte y garantizar la protección contra la vista de personas no autorizadas.

b) Si el dispositivo móvil de almacenamiento de datos debe dejarse desatendido en un vehículo, este debe estar cerrado con llave y el dispositivo debe estar fuera de la vista (preferiblemente en el baúl cerrado del vehículo).

C. Envío de dispositivos móviles de almacenamiento de datos de propiedad estatal

Los dispositivos móviles de almacenamiento de datos que contengan información crítica o restringida pueden enviarse cuando se cumplan las siguientes condiciones:

1. Se utiliza cinta adhesiva, sellador u otro material que evidencie la manipulación para identificar una brecha en el paquete; y

2. Se identifican las personas que tienen necesidad de conocer sobre el envío.

a) Se autorizan los nombres de los receptores previamente acordados para la firma al momento de la entrega.

b) Se garantiza la confirmación de la entrega al destinatario en el momento de la entrega (por ejemplo, el destinatario se comunica con el remitente a la llegada del paquete).

c) Las contraseñas se identifican en una comunicación separada. El personal no puede identificar la contraseña relacionada en la misma comunicación que menciona el dispositivo móvil de almacenamiento de datos específico.

D. Deben respetarse los acuerdos intergubernamentales sobre el intercambio de información restringida o crítica en los dispositivos móviles de almacenamiento de datos.

E. Eliminación de los dispositivos móviles de almacenamiento de datos

1. El personal debe entregar o enviar por correo los dispositivos móviles de almacenamiento de datos de la OYA al servicio de atención al usuario de los Servicios de Información para su eliminación.

2. Los Servicios de Información deben seguir la política estatal de Adquisición y eliminación sostenible de equipos electrónicos (política del DAS 107-009-0050).

3. Cuando se envíe por correo postal, el personal debe notificar al servicio de atención al usuario de los Servicios de Información por correo electrónico el número de dispositivos y la fecha de envío.

4. Los Servicios de Información deben confirmar la recepción y destrucción de los dispositivos.

VIII. PROTOCOLO DE FUNCIONAMIENTO LOCAL REQUERIDO: NO