CORRECCIONAL JUVENIL DE OREGON

Declaración de la política

Parte I: servicios administrativos

Asunto:

Respuesta a incidentes de seguridad de la información

Sección – Número de política:	*Sustituye a:*	*Fecha de entrada en vigencia:*	*Fecha de la última revisión/ actualización:*
E: gestión de la información – 3.3	**I-E-3.3 (08/19)** **I-E-3.3 (12/14)** **I-E-3.3 (3/12)**	**10/29/2021**	**Ninguna**

Normas y referencias relacionadas:	▪ Estatutos Revisados de Oregon (Oregon Revised Statutes (ORS, por sus siglas en inglés)) 276A.300 (Seguridad de los sistemas de información en el departamento ejecutivo; normas) ▪ Política estatal del Departamento de Servicios Administrativos de Oregon (Department of Administrative Services (DAS, por sus siglas en inglés)) 107-004-120 Respuesta a incidentes de seguridad de la información ▪ Plan de respuesta a incidentes de seguridad de la información del estado de Oregon ▪ Política de la Correccional Juvenil de Oregon (Oregon Youth Authority (OYA, por sus siglas en inglés)): 0-7.0 Uso de activos y sistemas de información electrónicos I-C-9.0 Dispositivos móviles de comunicación (celulares) y otros dispositivos móviles de almacenamiento de datos I-E-1.0 Notificación e informe de incidentes del director I-E-3.2 Clasificación y protección de activos de información I-E-2.0 Conservación, destrucción y archivo de registros I-E-2.1 Solicitudes de registros públicos para los registros de la agencia I-E-2.2 Protección y transferencia de archivos de casos y archivos médicos de la correccional I-E-2.3 Solicitudes de información y registros de los jóvenes ▪ Política del Sistema de Información de Justicia Juvenil (Juvenile Justice Information System (JJIS, por sus siglas en inglés)): privacidad y protección de la información confidencial en el JJIS ▪ Formulario de la OYA: YA 1970 Respuesta a incidentes de seguridad de la información ▪ Matriz de clasificación y protección de activos de información de la OYA ▪ Plan de respuesta a incidentes de seguridad de la información de la OYA
Procedimientos relacionados:	▪ TS I-E-3.3 Respuesta a incidentes de seguridad de la información del servicio de atención al usuario

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

I. PROPÓSITO:

Esta política establece las capacidades de respuesta a incidentes de seguridad de la información de la OYA para proporcionar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Los incidentes de seguridad de la información abarcan desde las intrusiones no autorizadas en los sistemas de red de la OYA hasta el mal manejo de la información que puede poner en riesgo su confidencialidad, integridad o disponibilidad. La política también garantiza una investigación adecuada de los incidentes de pérdida, daño, uso incorrecto o difusión inadecuada de activos de información.

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: cualquier conocimiento que pueda comunicarse o material documental, independientemente de su forma física o de sus características, incluyendo la comunicación electrónica, en papel y verbal.

Seguridad de la información: conservación de la confidencialidad, integridad y disponibilidad de la información. También pueden intervenir otras características como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

Evento de seguridad de la información: suceso observable y medible con respecto de un activo de información que constituye una desviación de las operaciones normales.

Incidente de seguridad de la información (incidente): un evento único o una serie de eventos de seguridad de la información no deseados o inesperados que resultan en un daño, o plantean una amenaza significativa de daño a los activos de información, a la OYA o a un tercero y requieren una medida preventiva o correctiva no rutinaria.

Plan de respuesta a incidentes de seguridad de la información: documento escrito que establece el enfoque para abordar y gestionar los incidentes de seguridad de la información.

Equipo de seguridad de la información: empleados de la OYA responsables de supervisar el programa de seguridad de la información de la agencia para ayudar a garantizar a que se aborden los objetivos de seguridad. Los miembros del equipo incluyen al director de información de la OYA, el director de seguridad de los servicios de información, el funcionario de gestión de expedientes y el coordinador de normas/políticas. (Consulte el plan de seguridad de la información de la OYA para obtener más información).

Director de seguridad de los Servicios de Información (Information Services Security Officer (ISSO, por sus siglas en inglés)): empleado de la OYA que es responsable de la gestión de las políticas y prácticas de la agencia relacionadas con la seguridad de los activos de información electrónica.

Información restringida: información sensible 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.

III. POLÍTICA:

La OYA tiene un programa de respuesta a incidentes para responder a los incidentes de seguridad de la información de forma electrónica, en papel o verbalmente. El programa consiste en el plan de respuesta a incidentes de seguridad de la información de la OYA, los procedimientos de respuesta a incidentes, esta política, la capacitación de concienciación del personal y la revisión continua. El personal debe seguir el plan de respuesta a incidentes de seguridad de la información de la OYA siempre que se sospeche o se produzca un incidente de seguridad de la información.

Todas las personas que tengan acceso a la información o a los sistemas de la OYA deben cumplir con esta política y con las políticas, procedimientos y directrices relacionados. Estas personas incluyen al personal de la OYA, los voluntarios, los contratistas, los trabajadores temporales, las personas empleadas por otros para realizar el trabajo de la OYA y otras personas autorizadas con acceso a la información, las redes o los sistemas de la OYA.

El personal debe informar inmediatamente de forma verbal sobre los eventos de seguridad de la información a sus supervisores o al oficial del día (officer-of-the-day (OD, por sus siglas en inglés), **y** al servicio de atención al usuario de los Servicios de Información (503) 378-4333. Se aceptan los mensajes de voz.

Los incidentes de seguridad de la información verificados se consideran incidentes significativos y requieren un Informe de incidentes del director conforme a la política de la OYA I-E-1.0 (Notificación e informe de incidentes del director).

IV. NORMAS GENERALES:

A. El director de seguridad de los Servicios de Información (ISSO, por sus siglas en inglés) es el punto de contacto de incidentes (Incident Point of Contact (IPOC, por sus siglas en inglés)), relacionado con la seguridad de la información de la agencia.

B. Plan de respuesta a incidentes de seguridad de la información

La OYA tiene un plan de respuesta a incidentes para responder a los incidentes de la agencia. El plan incluye funciones, responsabilidades, procesos y procedimientos para manejar los incidentes de seguridad de la información.

C. Informe de eventos de seguridad de la información

Un evento de seguridad de la información que se debe informar por estar relacionado con la seguridad de la información (consulte la definición); no deseado, inesperado o accidental; muestra daño, intención de daño o amenaza significativa de daño; o la respuesta requiere una acción no rutinaria.

1. El personal debe informar inmediatamente de forma verbal sobre los eventos de seguridad de la información a sus supervisores o al oficial del día (officer-of-the-day (OD, por sus siglas en inglés)), y al servicio de atención al usuario de los Servicios de Información al (503) 378-4333. Se aceptan los mensajes de voz.

   El personal también debe informar del evento por correo electrónico a IS.WorkOrder@oya.state.or.us, indicando en el asunto “Information Security Event” [Evento de seguridad de la información].

2. El personal debe incluir la siguiente información en sus informes:

   a) La naturaleza del evento;

   b) La información que está en riesgo;

   c) Si existe algún riesgo adicional; y

   d) Las iniciativas de mitigación que se han realizado, si las hay.

3. Tras la notificación de un evento, el personal del servicio de atención al usuario de los Servicios de Información debe comunicarse inmediatamente con el IPOC.

4. El IPOC debe evaluar la vulnerabilidad, el riesgo y la posible clasificación del evento como incidente de seguridad de la información, de acuerdo con el plan de respuesta a incidentes de seguridad de la información de la OYA.

Los posibles incidentes de seguridad de la información serán evaluados utilizando un formulario YA 1970 Respuesta a incidentes de seguridad de la información.

5. Si el evento es clasificado como un incidente de seguridad de la información, el IPOC debe compartir el incidente con los Servicios de Ciberseguridad y el Equipo de Seguridad de la Información (Information Security Team (IST, por sus siglas en inglés)) de la OYA en un plazo de 24 horas a partir del suceso.

   a) El IPOC debe comunicarse con el IST para clasificar, valorar y determinar cómo responder al incidente.

   b) El IPOC debe seguir la política de la OYA I-E-1.0 (Notificación e informe de incidentes del director).

   c) El IPOC debe coordinarse con los Servicios de ciberseguridad (Cyber Security Services (CSS, por sus siglas en inglés)) según el plan de respuesta a incidentes de seguridad de la información del estado de Oregon. Puede comunicarse con ellos al (503) 378-5930 o a ESO.SOC@oregon.gov.

   d) Los miembros del equipo ejecutivo de la OYA deben proporcionar recursos adicionales para mitigar y responder a un incidente cuando sea necesario.

   e) Al menos una vez al año, el IST debe presentar los datos sobre incidentes y eventos de seguridad de la información al equipo ejecutivo para la concienciación, la revisión de las tendencias, la capacitación y los problemas con la política.

D. Los ejemplos de eventos de seguridad de la información que deben notificarse incluyen, pero no se limitan a:

1. La información personal se divulga accidental o intencionadamente a personas no autorizadas (por ejemplo, el nombre o la inicial del nombre y el apellido de la persona ***y*** el número de Seguro Social, el número de identificación, el número de cuenta, el número de la tarjeta de crédito, el número de la tarjeta de débito);

2. Una persona no autorizada solicita o recibe acceso a los sistemas de la OYA;

3. La contraseña de las redes y de los sistemas de la OYA, o el acceso al JJIS se encuentran comprometidos;

4. La reproducción no autorizada de la información;

5. Las personas no autorizadas se encuentran en el área restringida;

6. Los documentos de información restringida o crítica no se destruyen adecuadamente;

7. La pérdida o robo de datos físicos o electrónicos que contienen información restringida o crítica;

8. Los documentos de información restringida o crítica no están protegidos o no se manejan adecuadamente;

9. Se pierde o roban un dispositivo de comunicación móvil u otro dispositivo de almacenamiento de datos (por ejemplo, una computadora portátil, un teléfono inteligente, una unidad de memoria flash, un CD, una estación de trabajo de escritorio) que contiene información restringida o crítica;

10. Los datos se anulan o se destruyen;

11. Una persona no autorizada que divulga información al público al escuchar una conversación sobre información restringida o crítica;

12. Los datos se modifican por razones inexplicables; o

13. Cualquier violación de las políticas de seguridad de la información de la OYA.

E. Los ejemplos de eventos de seguridad de la información que no deben notificarse incluyen, pero no se limitan a:

1. Las violaciones por delitos sin componentes de seguridad de la información, como el robo de un carro (no implica a la seguridad de la información);

2. La red o intranet no está disponible debido a un problema o mantenimiento de rutina (la medida necesaria es de rutina);

3. La pérdida de un maletín que contiene información de acceso público (no hay daño, ni intención de daño, ni amenaza significativa de daño); o

4. Se detecta un virus informático en una estación de trabajo que se contiene con éxito por el software antivirus (la medida necesaria es de rutina).

5. Si el personal no está seguro de si una situación se debe informar, se le anima a ser precavido e informarla.

F. El coordinador de voluntarios de la OYA y los administradores de contratos deben asegurarse de que los voluntarios y contratistas conozcan y sigan esta política, cuando sea aplicable.

G. El IST se asegurará de que el proceso de denuncia se pruebe al menos una vez al año para evaluar la concienciación del personal y la vulnerabilidad de la agencia.

H. Los servicios de información deben contar con un procedimiento escrito para toda la agencia que defina cómo el personal del servicio de atención al usuario responderá y documentará los eventos e incidentes de seguridad de la información notificados por el personal.

V. PROTOCOLO DE FUNCIONAMIENTO LOCAL REQUERIDO: NO