SAGRADO
Universidad del Sagrado Corazón

Política para el Acceso a la Información Electrónica

Efectivo: 2019.07.01

Propósito

Sagrado (también conocido como "Universidad") establece esta Política que aplica al acceso a información transmitida por o almacenada en los medios electrónicos. El acceso debe ocurrir solo para un propósito legítimo y autorizado por uno o más oficiales autorizados y limitado a la información electrónica mínima necesaria para lograr el propósito. En general, la Universidad no divulga información electrónica a un tercero sin el consentimiento del usuario, excepto cuando la Universidad está sujeta a un proceso legal en cuyo caso la Universidad hará los esfuerzos razonables para notificar al usuario.

Aplicabilidad

Esta Política aplica a todos los estudiantes universitarios, facultad regular y parcial, empleados administrativos y de propuestas y a otros ("usuarios") con acceso y uso de los recursos de tecnología e información ("IT") de Sagrado.

Definiciones

Acceso. La verificación, uso o divulgación de contenido o actividad de datos que va más allá del contacto incidental con información diseminada por o almacenada en medios electrónicos de los recursos de tecnología e información (IT) de la Universidad. Para evitar la duda, la mera conservación de información en los sistemas electrónicos no es considerada como acceso hasta que ocurre una verificación o divulgación.

Oficial Autorizado. Los oficiales autorizados incluyen: Presidente, Vicepresidente Ejecutivo de Asuntos Académicos, Asesor Legal General, Vicepresidente de Asuntos Estudiantiles, Vicepresidente de Finanzas y Operaciones, Vicepresidente de Desarrollo Organizacional y Recursos Humanos, según sea apropiado y dependiendo del racional para acceder información electrónica. Cada uno de estos oficiales autorizados puede nombrar un suplente para autorizar el acceso en aquellas circunstancias donde el oficial autorizado no se encuentre disponible.

Información Electrónica. La Información electrónica consiste en dos tipos de información:

1. Contenido: Archivos creados en, transmitidos a través de o almacenados en los recursos de IT de la Universidad, incluyendo información para la cual los usuarios crean una copia de seguridad en los recursos de IT de la Universidad desde máquinas que sean propiedad del usuario.
2. Datos de Actividad**:** Datos generados automáticamente por los recursos de informática de la Universidad incluyendo registro de uso de Internet o entradas que son accesibles desde los sistemas mantenidos por la Universidad o sus agentes.

Circunstancias de emergencia. Circunstancias en las que el factor tiempo es esencial y la Universidad necesita actuar de inmediato para evitar pérdida o daños significativos a la propiedad.

Notificación de solicitud de terceros. Aviso al usuario de una solicitud hecha por un tercero para acceder o divulgar información electrónica antes de la divulgación de dicha información (por ejemplo, orden judicial, citación judicial, orden judicial, investigación gubernamental o un litigio que involucre a la Universidad).

Investigación de la Universidad. Alegación o querella que requiere que se investigue una posible violación a la ley o a una política de la Universidad. La investigación de la Universidad también incluye una auditoría interna y externa.

Recursos de informática de la Universidad. Todas las máquinas de computación y comunicación, los servicios, redes y otras tecnologías que se usan para acceder, almacenar o transmitir información personal o de la Universidad y que son propiedad, son provistas o son administradas por o a través de la Universidad, independientemente de que sean propiedad de o controladas por la Universidad o por un proveedor externo de servicios electrónicos contratados por la Universidad.

Usuario. Cualquier persona o entidad que use los recursos de IT de la Universidad para crear, descargar, almacenar, transmitir o procesar cualquier tipo de información.

Consentimiento de Usuario. Cuando un usuario da su consentimiento para el acceso, uso y / o divulgación de la información electrónica de la Universidad siguiendo una descripción del propósito y el alcance de una solicitud de acceso a la información electrónica.

Privacidad y Confidencialidad

1. Introducción

Los usuarios no deben tener una expectativa de privacidad en las comunicaciones transmitidas o almacenadas en los recursos de IT de la Universidad. Sin embargo, en la medida permitida por la ley y la política de la Universidad, Sagrado mantiene y protege tanto la privacidad de las personas como la confidencialidad de la información oficial almacenada en sus sistemas de tecnología de la información.

2. Información Disponible a la Universidad

La Universidad puede acceder a la información electrónica generada por el usuario. Incluso cuando se utilizan dispositivos de propiedad personal, las interacciones del usuario con los recursos informáticos de la Universidad generan datos de actividad que a menudo se pueden atribuir a un individuo al tiempo que se identifica la ubicación física de esa persona con diversos grados de precisión. Los usuarios deben saber que la Universidad tiene o podría tener acceso a muchas categorías de información.

En el transcurso de su tiempo en Sagrado, los usuarios podrían estar involucrados en circunstancias en las que la Universidad podría acceder legítimamente a la información electrónica. La Universidad aconseja a los usuarios que utilizan los recursos de IT de la Universidad para asuntos personales que la Universidad podría acceder a la información electrónica relacionada con los asuntos bajo esta Política.

Incluso bajo circunstancias en las cuales la Universidad puede legítimamente preservar, monitorear o acceder a la información electrónica bajo esta Política, no revelará dicha información electrónica a terceros sin una notificación de la solicitud de un tercero o el consentimiento del usuario, a menos que (a) hacerlo por ley o por un proceso legal; (b) para proteger la vida o la propiedad; (c) durante el curso de una investigación de mala conducta, violaciones de la ley o violaciones de la política de la Universidad por parte de estudiantes o empleados; o (d) para reportar un crimen relacionado o indicado por la información electrónica.

3. Obligación de Privacidad de los Empleados y Agentes de la Universidad

Esta Política prohíbe que los empleados, universitarios y sus agentes accedan a la información electrónica, excepto de conformidad con esta Política. Los empleados de la universidad deben tomar las precauciones necesarias para proteger la confidencialidad de la información personal encontrada ya sea en el desempeño de sus funciones o de otra manera. Los contratos universitarios con proveedores externos que tendrán acceso a información electrónica identificable personalmente incluirán referencias a esta Política, o a las leyes de privacidad aplicables que protegen la información, o el lenguaje

que limita al contratista tercero el uso de la información para cualquier fin que no sea realizar los servicios del acuerdo, o según lo exija la ley.

Si se ha accedido a la información electrónica de un usuario en violación de esta Política, el/ella debe ser notificada de inmediato. Cuando dicha violación a la Política también requiera una notificación legal conforme a una ley aplicable, el aviso legal servirá como la notificación requerida en esta sección.

4. Conversaciones por Audio o Video

En cumplimiento con la ley, las conversaciones no se registrarán ni se supervisarán sin avisar a todos los participantes, a menos que un tribunal haya ordenado explícitamente que tal monitoreo o registro ocurra sin previo aviso. Los servicios de emergencia deben registrar las llamadas de emergencia de tipo 911 de acuerdo con las leyes y regulaciones federales y estatales. Las personas que llaman deben ser informadas cuando una llamada está siendo monitoreada o registrada con el propósito de evaluar el servicio al cliente, evaluar la carga de trabajo o cualquier otro propósito comercial permitido por la ley.

Acceso Sin Consentimiento del Usuario

En general, la Universidad obtendrá el consentimiento del usuario antes de cualquier acceso, excepto en las condiciones que se describen a continuación. Al acceder a una información electrónica sin el consentimiento del usuario, al menos un funcionario autorizado debe solicitar, documentar y aprobar el acceso por escrito.

1. Protección, Mantenimiento o Manejo del Sistema

Los recursos de IT de la Universidad requieren mantenimiento e inspección continuos para garantizar que funcionen correctamente para garantizar que cumplan con las obligaciones reglamentarias y contractuales y para protegerse de las amenazas a la seguridad, como los ciberataques, el malware y los phishing. Los recursos de IT de la Universidad también requieren una administración regular, por ejemplo, para implementar actualizaciones de software. En consecuencia, para realizar este trabajo, la Universidad y sus proveedores aprobados pueden escanear o acceder a información electrónica sin el consentimiento del usuario.

El Principal Oficial de Información (CIO) puede autorizar el acceso para la protección, el mantenimiento y la administración del sistema. En ese proceso, el personal de la Oficina de Tecnología e Información Integrada (ITI) puede observar ciertos datos de actividad u otra información electrónica.

Excepto lo dispuesto en otra parte de esta Política o por ley, el personal de ITI no puede buscar información electrónica, incluidos los contenidos o los datos de actividad, cuando no guarde relación con las operaciones y el soporte del sistema. Cualquier examen inevitable de información electrónica se limitará al mínimo requerido para realizar tales tareas; siempre que, sin embargo, esta excepción no signifique que el personal de ITI pueda usar o divulgar información personal o confidencial sin la autorización escrita de un funcionario autorizado.

Si, durante sus funciones, un personal de ITI descubre inadvertidamente o sospecha violaciones a esta Política, la ley u otra política de la Universidad, dicho personal puede conservar los datos e informar tales violaciones al CIO.

2. Circunstancias de emergencia

La Universidad puede acceder a información electrónica sin el consentimiento del usuario en circunstancias de emergencia donde el tiempo es esencial (por ejemplo, acceder a la información de salud de un estudiante en una emergencia médica).

3. Investigaciones de la Universidad

La Universidad puede acceder y conservar acceso a información electrónica o monitorear cuentas y equipos sin el consentimiento del usuario para realizar una investigación universitaria de una presunta violación a esta Política, un requisito legal, mala conducta u otra política de la Universidad (por ejemplo, investigación de una queja de abuso sexual). mala conducta o intimidación utilizando el correo electrónico de la Universidad; investigación sobre el uso de recursos de IT para acceder a sitios web que pueden considerarse inapropiados u ofensivos).

4. Identidad del Usuario Desconocida

La Universidad puede acceder a información electrónica sin el consentimiento del usuario cuando se desconoce la identidad del usuario, y la Universidad está investigando una presunta violación de esta Política, un requisito legal, mala conducta u otra política de la Universidad.

5. Proceso legal

Las solicitudes de información electrónica derivadas de un proceso legal como órdenes de registro, órdenes judiciales, citaciones u otras demandas relacionadas con investigaciones gubernamentales o litigios de la Universidad deben remitirse al Asesor Jurídico General que autorizará el acceso y la divulgación de la información electrónica. bajo esta circunstancia.

La Universidad hará todos los esfuerzos razonables para notificar al usuario antes de acceder o divulgar la información electrónica y con aviso suficiente para permitirle al usuario objetar ante el tribunal la solicitud legal. En algunas circunstancias, se le podría prohibir a la Universidad divulgar la existencia de un proceso legal (por ejemplo, orden de un tribunal de justicia u organismo de aplicación de la ley dirigido a la Universidad para proporcionar información electrónica de un usuario para una investigación criminal) y la Universidad divulgará información del usuario de conformidad con dicho requisito legal sin previo aviso al usuario o su consentimiento.

Procedimiento para Acceder a Información Electrónica

El siguiente es el procedimiento para acceder a la información electrónica que está más allá del contacto incidental al proporcionar sistemas de IT de la Universidad, con o sin el consentimiento del usuario.

1. Autorización

Al menos un oficial autorizado debe solicitar, documentar y aprobar el acceso por escrito. El oficial autorizado correspondiente depende del usuario, la naturaleza de la información y la justificación para acceder a la información electrónica. Ejemplos: Presidente para cualquier usuario y tipo de información, Vicepresidente Ejecutivo de Asuntos Académicos para la facultad, Asesor Jurídico General para procesos legales, Vicepresidente de Asuntos Estudiantiles para estudiantes, Vicepresidente de Finanzas y Operaciones para proveedores, asuntos comerciales y financieros, Vicepresidente de Desarrollo Organizacional y Recursos Humanos para empleados administrativos. En caso de una emergencia, cualquier oficial autorizado puede solicitar, documentar y aprobar el acceso.

2. Notificación de Acceso Interno

El oficial autorizado notificará al usuario afectado de la acción tomada y los motivos de la acción tomada lo antes posible que sea legal y preserve la integridad de la investigación, a menos que la ley o política exija confidencialidad y por lo tanto impida la notificación.

3. Transparencia y Documentación

El oficial autorizado evaluará todas las circunstancias relevantes para determinar si autoriza el acceso y conservará un registro de la solicitud, el fundamento, la aprobación y el proceso que se siguió, incluidos, entre otros, los siguientes:

- descripción de la información electrónica que fue accedida;

- la justificación para el acceso;
- el proceso legal usado para obligar al acceso, si aplica;
- si el usuario fue notificado y si no, el fundamento para no notificar;
- si el usuario consintió y si no, los esfuerzos para obtener el consentimiento;
- documentos sobre la solicitud de información; y
- notificaciones de violaciones a la Política.

El CIO es responsable de mantener un registro de resumen no identificado de las instancias de acceso a la información electrónica.

Informar el Uso Indebido del Acceso a la Información Electrónica

Los usuarios tienen la responsabilidad de reportar sospechas de incidentes de uso indebido del acceso a la información electrónica incluyendo, pero sin limitarse a, sospechas de actividades ilícitas o impropias al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

Inspección y monitoreo la información y los recursos de IT pueden ser necesarios para cumplir con esta Política, realizar investigaciones o auditorías, garantizar la seguridad de una persona o de la Universidad, cumplir con la ley o garantizar el funcionamiento adecuado de los recursos de IT. Solo el CIO (o designado) puede autorizar esta inspección y monitoreo.

Se espera que los usuarios de los recursos de IT cooperen con cualquier investigación de abuso de Políticas y Procedimientos. La falta de cooperación puede ser motivo de cancelación de privilegios de acceso u otras medidas disciplinarias.

Consultas sobre esta Política

Las consultas sobre el alcance y la interpretación y las de esta Política deben dirigirse al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

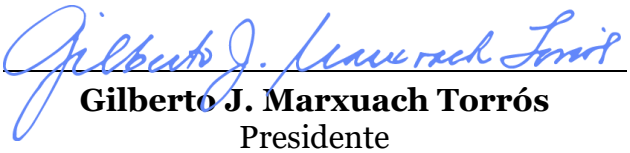
Denuncias de Violaciones a la Política

Las violaciones a esta Política deben dirigirse al Asesor Jurídico al 787.728.1515, ext. 1221, o por correo electrónico a cameliac.fernandez@sagrado.edu, o al Oficial de Cumplimiento e Integridad.

Violaciones a esta Política

La Universidad del Sagrado Corazón se reserva el derecho de interpretar esta Política en su administración, implementación y aplicación. Cualquier violación de esta Política por parte de un estudiante, profesorado o personal o cualquier otra persona puede resultar en una acción disciplinaria que puede incluir la expulsión de la Universidad (estudiantes) o la terminación de la relación laboral (personal docente y administrativo) u otras acciones legales apropiadas.

Si existe alguna ambigüedad en cualquier disposición de esta Política, la Universidad se reserva la discreción de interpretarla de acuerdo con el propósito para el cual fue establecida, el impacto en las operaciones de la Universidad y la buena fe, a menos que cualquier ley establezca lo contrario.



Gilberto J. Marxuach Torrós
Presidente