**Política de uso aceptable de información tecnológica**

**1.0 Descripción general**

Las intenciones del Departamento de Sistemas de Información (SI) de publicar una **Política de uso aceptable** continúa con la cultura de apertura, confianza e integridad establecida por la Universidad Politécnica de Puerto Rico (UPPR). El departamento de SI tiene el compromiso de proteger a los empleados de la UPPR y a la Institución de las acciones ilegales o perjudiciales que realicen los individuos, sea consciente o inconscientemente.

Los sistemas relacionados con la Internet / Intranet / Extranet incluyendo, pero no limitado a, equipo de cómputo, software, sistemas operativos, medios de almacenamiento, cuentas de red que proporcionan correo electrónico, navegación WWW y FTP, son propiedad de la UPPR. Estos sistemas deben ser utilizados con fines comerciales al servicio de los intereses de la Universidad en el curso de operaciones normales.

La seguridad efectiva es un esfuerzo de equipo que implica la participación y el apoyo de todos los empleados de la UPPR y sus afiliados que manejen información y/o sistemas de información. Es responsabilidad de cada usuario de computadora conocer estas directrices y llevar a cabo sus actividades de acuerdo con las mismas.

**2.0 Propósito**

El propósito de esta política es definir el uso aceptable de los equipos de computadora en la UPPR. Estas reglas se establecen para proteger a los empleados y a la UPPR. El uso inapropiado expone a la UPPR a riesgos, incluyendo ataques de virus, compromete sistemas de redes y servicios, y a cuestiones de índole legal.

**3.0 Ámbito de aplicación**

Esta política aplica a empleados, contratistas, consultores, empleados temporeros y otros trabajadores de la UPPR, incluyendo todo el personal afiliado con terceros. Esta política se aplica a todos los equipos que son propiedad o están arrendados por la UPPR, sea directa o indirectamente (subvenciones/”*grants”*).

**4.0 Política**

**4.1 Uso general y propiedad**

1. Aunque la administración de la red de la UPPR desea proporcionar un nivel razonable de privacidad, los usuarios deben ser conscientes de que los datos que se crean en el sistema institucional siguen siendo propiedad de la UPPR. Dada la necesidad de proteger la red de la UPPR, la administración no puede garantizar la confidencialidad de la información almacenada en cualquier dispositivo de la red que pertenece a la UPPR.
2. Los empleados son responsables de ejercer el buen juicio en cuanto a la razonabilidad de uso personal. Cada departamento es responsable de la creación de directrices sobre el uso personal de sistemas de Internet / Intranet / Extranet. En ausencia de tales políticas, los empleados deben regirse por las políticas departamentales de uso personal y, si hay alguna incertidumbre, deben consultar a su supervisor o gerente.
3. SI recomienda que toda la información que los usuarios consideren sensibles o vulnerables sea cifrada.
4. Para fines de seguridad y mantenimiento de la red, las personas autorizadas pueden monitorizar aparatos, sistemas y tráfico de red en cualquier momento dentro de la UPPR.
5. La UPPR se reserva el derecho de auditar las redes y los sistemas periódicamente para garantizar el cumplimiento de esta política.

**4.2 Seguridad e información privilegiada**

1. La interfaz de usuario para la información contenida en los sistemas relacionados con la Internet / Intranet / Extranet debe clasificarse como confidencial o no confidencial, según lo definido por las normas de confidencialidad de la UPPR; ver el aviso de confidencialidad de correo electrónico adjunto. Algunos ejemplos de información confidencial incluyen, pero no se limitan a, empresa privada, estrategias empresariales, sensibles al competidor, secretos comerciales, especificaciones, listas de clientes y datos de investigación. Los empleados deben tomar todas las medidas necesarias para evitar el acceso no autorizado a esta información.
2. Mantenga las contraseñas seguras y no comparta cuentas. Los usuarios autorizados son responsables de la seguridad de sus contraseñas y cuentas. Las contraseñas a nivel de sistema se deben cambiar trimestralmente, las contraseñas a nivel de usuario se deben cambiar cada seis meses.
3. Todas las computadoras personales, portátiles y estaciones de trabajo deben estar aseguradas con un protector de pantalla protegido por contraseña con la función de activación automática programada para 10 minutos o menos, o cerrando la sesión (por medio de *control-alt-delete* para los usuarios de Windows) cuando el nodo va a estar desatendido.
4. Dado que la información contenida en las computadoras portátiles es particularmente vulnerable, se debe ejercer un cuidado especial.
5. Todos los mensajes de los empleados originados desde una dirección de correo electrónico de la UPPR a grupos de interés deben contener la advertencia oficial que afirma que las opiniones expresadas son estrictamente suyas y no necesariamente las de la UPPR, a menos que el mensaje se realice en el ámbito de las funciones de la empresa.
6. A menos que prevalezca la política del departamento o grupo, todos los nodos utilizados por el empleado que están conectados a la Internet / Intranet / Extranet de la UPPR, ya sean propiedad del trabajador o de la UPPR, estarán continuamente ejecutando el software de detección de virus con una base de datos de virus actualizada.
7. Los empleados deben ejercer suma cautela al abrir anejos de correo electrónico recibidos de remitentes desconocidos que pueden contener virus, bombas de correo electrónico o el código de caballo de Troya.

**4.3. Uso inaceptable**

Las siguientes actividades están, en general, prohibidas. Los empleados pueden estar exentos de estas restricciones en el desempeño de sus responsabilidades legítimas de trabajo (por ejemplo, el personal de administración de sistemas pueden tener la necesidad de desactivar el acceso a la red de un nodo si el nodo está interrumpiendo los servicios de producción).

En ningún caso un empleado de la UPPR está autorizado para participar en una actividad que es ilegal bajo la ley local, estatal, federal o internacional, mientras utiliza los recursos que son propiedad de la UPPR.

Las listas que siguen continuación no son exhaustivas, pero intentan proporcionar un marco de referencia para las actividades comprendidas en la categoría de uso inaceptable.

**Sistema y actividades en la red**

Las siguientes actividades están estrictamente prohibidas:

1. Violar los derechos de cualquier persona o empresa protegidos por derechos de autor, secretos comerciales, patentes u otra propiedad intelectual o leyes o reglamentos similares, incluyendo, pero no limitado a, la instalación o distribución de productos "pirateados" u otros productos de software cuyos usos no están debidamente autorizados por la UPPR.
2. Realizar copia no autorizada de material con derechos de autor, incluyendo, pero no limitado a, la digitalización y distribución de fotografías de revistas, libros u otros recursos con derechos de autor, música con derechos de autor, y la instalación de cualquier software con derechos de autor para el cual la UPPR o el usuario final carece de licencia activa, está estrictamente prohibido.
3. Exportar software, información técnica, software o tecnología de cifrado, en violación a las leyes internacionales o regionales de control de exportación, es ilegal. Se debe consultar al departamento de SI previo a la exportación de cualquier material cuestionable.
4. Introducir programas maliciosos en la red o en el servidor (por ejemplo, virus, gusanos, caballos de Troya, bombas de correo electrónico, etc.)
5. Revelar su contraseña de la cuenta a los demás o permitir el uso de su cuenta a otras personas. Esto incluye la familia y otros miembros del hogar cuando se trabaje desde la casa.
6. Utilizar un activo informático de la UPPR para participar activamente en la adquisición o transmisión de material que está en violación de las leyes de acoso sexual o leyes de hostilidad en el lugar de trabajo en la jurisdicción local del usuario. Consulte el Título VII de la Ley de Derechos Civiles de 1964, enmendada, la Discriminación por Edad en el Empleo de 1967 y la Ley para Estadounidenses con Discapacidades de 1999.
7. Hacer ofertas fraudulentas de productos, artículos o servicios procedentes de cualquier cuenta de la UPPR.
8. Provocar brechas de seguridad o interrupciones de comunicación en la red. Las brechas de seguridad incluyen, pero no están limitadas a, acceder datos que el empleado no está destinado a recibir o conectarse a un servidor o cuenta para el cual el empleado no está expresamente autorizado a acceder, a menos que estas responsabilidades estén dentro del ejercicio regular de sus funciones. Para propósitos de esta sección, "interrupción" incluye, pero no está limitado a, husmear la red (*network sniffing*), ataques de inundación (*pinged floods*), falsificación de paquete/suplantación de IP (*packet spoofing)*, denegación de servicio e información de enrutamiento (*routing)* falsificada con propósitos maliciosos.
9. Escanear puertos o realizar escaneos de seguridad está expresamente prohibido, queda supeditad

a la gestión adecuada, previa notificación y aprobación de la oficina de SI.

1. Ejecutar cualquier forma de supervisión de la red que intercepte los datos no destinados para el nodo del empleado, a menos que esta actividad forme parte del trabajo normal del empleado.
2. Eludir la autenticación o la seguridad de cualquier nodo, red o cuenta.
3. Interferir con o denegar el servicio a cualquier usuario que no sea del nodo del empleado (por ejemplo, ataque de denegación de servicio).
4. Usar cualquier programa o secuencia de comandos (*script*) /comando o el envío de mensajes de cualquier tipo, con la intención de interferir con o deshabilitar la sesión del terminal del usuario, a través de cualquier medio, sea a nivel local o a través de la Internet/Intranet/Extranet.

**Correo electrónico y actividades de comunicación**

1. Enviar mensajes no solicitados de correo, incluyendo el envío de "correo basura" o material publicitario a individuos que no solicitaron específicamente dicho material (“correo basura”).
2. Cualquier forma de acoso o violación de las leyes federales y estatales a través de correo electrónico, teléfono, ya sea a través del lenguaje, frecuencia o tamaño de los mensajes.
3. El uso no autorizado o falsificación de la información del encabezado de correo electrónico.
4. Solicitar correo electrónico para moverlo (forward) cualquier otra dirección de correo electrónico, para una cuenta distinta a la del remitente, con la intención de acosar o recabar respuestas.
5. Crear o enviar "cartas en cadena", "Ponzi" u otros esquemas piramidales de cualquier tipo.
6. Utilizar correo electrónico no solicitado procedente de las redes de la UPPR a nombre de otros proveedores de servicios de Internet/Intranet/Extranet o para anunciar cualquier servicio hospedado por la UPPR o conectado a través de la red de la UPPR.
7. Publicar los mismos mensajes no comerciales o similares a un gran número de grupos de noticias de Usenet .

**El acoso (acoso cibernético)**

Ningún miembro de la comunidad puede utilizar los recursos institucionales para la difamación, calumnia, o acosar a cualquier otra persona. El acoso incluye, sin limitación, los siguientes:

1. Utilizar recursos institucionales con el fin de molestar, acosar, aterrorizar, intimidar, amenazar, ofender o molestar a otra persona mediante la transmisión de lenguaje obsceno, imágenes u otros materiales o amenazas de daño corporal al destinatario o de otros;
2. Utilizar los recursos institucionales para ponerse en contacto con otra persona con la intención de molestar, acosar o molestar, si no se comunica ningún mensaje real, y / o donde no existe propósito de la comunicación legítima, y ​​en el que el destinatario ha expresado su deseo para la comunicación de cesar;
3. Utilizar los recursos institucionales para ponerse en contacto con otra persona en relación con un asunto en el que uno no tiene el derecho legal de comunicar, una vez que el destinatario haya proporcionado un aviso razonable de que él o ella desea dicha comunicación a cesar;
4. Utilizar los recursos institucionales para perturbar o perjudicar a los miembros de la comunidad académica.
5. Utilizar los recursos institucionales para invadir la privacidad, académica o de otra manera, de otra, o la amenaza de invasión de la privacidad de otra.

**5.0 Aplicación**

Cualquier empleado que haya violado esta política puede estar sujeto a una acción disciplinaria, hasta e inclusive la terminación del empleo. Consulte el manual del empleado de la UPPR para más información.

**Aviso de confidencialidad**

**Aviso de confidencialidad**:

Esta es una comunicación privilegiada y confidencial de la Universidad Politécnica de Puerto Rico (el remitente y la persona a quien va dirigida la misma). Cualquier uso del contenido del mensaje por una persona a quien no se dirige el mismo es ilegal y está estrictamente prohibido. Ninguna persona podrá divulgar, copiar o alterar el contenido de este mensaje.  Si usted recibió esta comunicación por error, favor de destruirla junto con los anejos que haya podido tener la misma.