ESTÁNDARES PARA LA UTILIZACIÓN ACEPTABLE DE RECURSOS DE TECNOLOGÍA INFORMÁTICA

UNIVERSIDAD DE PUERTO RICO

Emitido el 4 de abril de 2008

Aprobado por:

Emma Fernández-Repollet, Ph.D.
Vicepresidenta de Investigación y Tecnología

4/7/08
Fecha

TABLA DE CONTENIDO

INTRODUCCIÓN A LA UTILIZACIÓN DE TECNOLOGÍA INFORMÁTICA 1

FUENTES DE REFERENCIA 1

ADQUISICIÓN Y ADMINISTRACIÓN DE LOS RECURSOS INFORMÁTICOS 1

UTILIZACIÓN DE LOS EQUIPOS INFORMÁTICOS Y PROGRAMAS 2

PROTECCIÓN DE LOS RECURSOS INFORMÁTICOS 2

UTILIZACIÓN DE LAS CLAVES DE ACCESO Y CONTRASEÑAS 3

ADMINISTRACIÓN DE LOS DOMINIOS 3

ACCESO SEGURO A LA RED DE COMUNICACIÓN 4

ACCESO SEGURO A LA RED INALÁMBRICA 4

PROTECCIÓN DE LOS DATOS PRIVADOS 5

ELIMINACIÓN SEGURA DE LOS DATOS 5

COMPARTIR ARCHIVOS ELECTRÓNICOS 5

DISEÑO DE LAS PÁGINAS WEB Y APLICACIONES DE INTERNET 6

EDUCACIÓN EN LA UTILIZACIÓN CORRECTA DE LA TECNOLOGÍA 6

REVISIÓN DE LOS ESTÁNDARES, GUÍAS Y PROCEDIMIENTOS 7

DEFINICIONES 8

HISTORIAL DE REVISIONES 14

INTRODUCCIÓN A LA UTILIZACIÓN DE TECNOLOGÍA INFORMÁTICA

La información contenida en este documento está subordinada y sujeta a la Certificación Núm. 35, Serie 2007-2008, de la Junta de Síndicos: *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico* ("la Política"). Todos los usuarios y administradores deben cumplir cabalmente con los Estándares estipulados en este documento. Cumplimiento con los mismos asegura el cumplimiento con la Política IT; y habilita que se haga el mejor uso posible de las tecnologías disponibles a la Universidad.

Todas las guías y procedimientos de tecnología a través de la Universidad deberán alinearse con la Política IT y con estos Estándares. La interpretación final sobre el significado, intención y enfoque hacia el cumplimiento de la Política y de estos Estándares radica con la Vicepresidencia de Investigación y Tecnología.

FUENTES DE REFERENCIA

Varias fuentes de información han sido utilizadas como insumo para este documento, para garantizar su entereza. Estos incluyen las políticas y guías existentes en otras universidades tanto dentro como fuera de los Estados Unidos, las leyes aplicables a nivel federal y estatal, mejores prácticas de expertos reconocidos en la industria y otras fuentes arbitradas.

ADQUISICIÓN Y ADMINISTRACIÓN DE LOS RECURSOS INFORMÁTICOS

La OSI identificará las especificaciones mínimas para adquirir equipos y programas informáticos; y hará estas especificaciones disponibles a la comunidad universitaria. Los usuarios y administradores utilizarán estas especificaciones cuando soliciten comprar computadoras y programas. Por la naturaleza particular del trabajo que le rinden a la Universidad, los investigadores podrán decidir si utilizan o no tales especificaciones.

Se deberá coordinar a través de la OSI cualquier adquisición e instalación de equipos y programas (incluyendo sistemas operativos) que habrán de ser apoyados por la OSI. Esto permitirá confirmar de antemano que la OSI tiene los recursos necesarios para brindar tal apoyo.

Como regla general, la industria informática establece la vida útil de los equipos en término de los años durante los cuales podrá ser utilizado productivamente por una institución. Todos los recintos, departamentos y oficinas deben contemplar la vida útil de su equipo al momento de revisar sus presupuestos anuales; de modo que puedan planificar apropiadamente la sustitución de los mismos en su debido momento, suponiendo que haya fondos disponibles para tal propósito. Según le sea requerido, la OSI podrá suministrar asesoría en identificar la edad, especificaciones técnicas y costo estimado de reemplazo de los equipos a ser sustituidos.

El determinante final en cuanto al tiempo que un equipo pueda ser utilizado es el cuidado y mantenimiento preventivo que se le brinde al mismo; y el apoyo que esté disponible a través de

las OSI o de la propia industria informática. La decisión de adquirir un equipo nuevo en lugar de reparar el existente se deberá basar en cuál de las dos alternativas le cuesta menos a la Universidad. La decisión de adquirir un equipo en lugar de reparar el existente deberá ser autorizada por el director de la oficina o laboratorio.

Todo equipo y programa informático adquirido a través de la Universidad se considera propiedad exclusiva de la Universidad. Las adquisiciones de tecnología se harán en cumplimiento con la Política IT y con la Certificación # 62, Serie 1994-1995, de la Junta de Síndicos: *Reglamentación para el Control de Activos Fijos en la Universidad de Puerto Rico*.

La adquisición de programas se hará en cumplimiento con la Política IT. Programas que no sean estándares se podrán adquirir según su necesidad, siguiendo la Política IT y las reglamentaciones y procedimientos pertinentes para adquirir equipo, suministro y servicios no-personales en la Universidad de Puerto Rico.

Los recintos, oficinas y facultades podrán transferir equipo productivo y licencias de programas entre sí, siguiendo los procedimientos de control correspondientes. Esto permitirá maximizar la utilización de recursos que aún tengan utilidad para la Universidad de manera eficiente. Equipo averiado podrá ser reparado mientras sea económicamente viable para la Universidad. De lo contrario, se dispondrá del mismo en cumplimiento con las reglamentaciones aplicables a la disposición de activos fijos en la Universidad de Puerto Rico.

UTILIZACIÓN DE LOS EQUIPOS INFORMÁTICOS Y PROGRAMAS

Los recursos informáticos que suministra la Universidad, tales como computadoras y redes de comunicación, serán utilizados solamente para propósitos autorizados. Cada usuario o administrador utilizará sólo aquel equipo o programa al cual tiene acceso legítimo. Ningún usuario o administrador incurrirá, fomentará, causará, asistirá o permitirá que se lleve a cabo una acción que resulte en un daño o perjuicio a los equipos y redes de comunicación, sistemas, aplicaciones o datos que le pertenecen a la Universidad. Esto incluye el llevar a cabo actividades que puedan interrumpir el trabajo legítimo que otros usuarios deban ejecutar para beneficio de la Universidad.

Evite hacer cambios no aprobados a la configuración del equipo y programas que le han sido asignados; puesto que impactará el funcionamiento de los mismos y su conectividad a la red.

El usuario o administrador deberá trancar o desconectarse de su computadora cuando deba apartarse de su área de trabajo; para evitar que terceros accedan a la misma sin autorización.

PROTECCIÓN DE LOS RECURSOS INFORMÁTICOS

Con el propósito de asegurar los recursos tecnológicos de la Universidad, los usuarios y administradores deberán tomar las medidas pertinentes para proteger las computadoras, servidores, redes de comunicación, aplicaciones y datos. Tales medidas deben incluir la

disponibilidad de facilidades especiales para ubicar el equipo en áreas que controlen su temperatura, humedad y control de acceso, según el nivel de criticidad de estos equipos. Terceros que deseen conectar sus equipos a la red universitaria deberán proveer protección similar a sus equipos para no comprometer la seguridad de la red.

Los programas maliciosos representan un riesgo sustancial a la Universidad en términos de tiempo, dinero y posible pérdida de programas y datos. Como parte del esfuerzo para proteger todo el equipo que acceda a los datos de la Universidad, toda computadora y servidor que se conecte a la red universitaria deberá mantener una versión actualizada de programas de protección tales como antivirus, anti-spyware o programas para detección de intrusos; configurados de acuerdo a los procedimientos pertinentes. Los usuarios y administradores aplicarán periódicamente las actualizaciones de dichos programas que hayan sido emitidas por los suplidores a las computadoras, servidores, redes, sistemas, aplicaciones y datos. Los administradores de servidores y equipo de red tomarán los pasos necesarios para aplicar las actualizaciones sin impactar o interrumpir la disponibilidad del servicio a los usuarios.

Los usuarios y administradores deberán resguardar las aplicaciones y datos periódicamente; de modo que puedan recuperarse en un tiempo mínimo en caso de alguna emergencia.

UTILIZACIÓN DE LAS CLAVES DE ACCESO Y CONTRASEÑAS

La combinación de clave de acceso (clave de usuario, User ID) y contraseña se asigna de forma única y exclusiva a cada usuario o administrador, como mecanismo para asegurar que solamente aquel usuario legítimo pueda acceder los datos y sistemas de la Universidad a través de la red de comunicación. Los usuarios y administradores tomarán las medidas que sean necesarias para proteger su clave de acceso y contraseña, ya sea que accedan de forma local o remota, en cumplimiento con la Política, estos Estándares, y las guías y procedimientos subordinados que sean implantados a través de la Universidad. Las contraseñas serán diseñadas siguiendo las técnicas de fuerza suministradas en las *Normas de Seguridad* de *la Oficina de Sistemas de Información*, para mitigar la posibilidad de acceso no autorizado.

ADMINISTRACIÓN DE LOS DOMINIOS

La Universidad y sus Recintos han establecido una presencia virtual en el Internet a través de sus dominios. La OSI Sistémica en Administración Central administra y opera el Sistema Denominacional de Dominios (DNS, por sus siglas en inglés) de la Universidad de Puerto Rico para el Internet, conocido como UPR.EDU y el bloque de direcciones IP asignado a éste. Quien desee definir un dominio adicional para que ejecute sobre la red sistémica deberá tramitar la autorización para dicho dominio con la OSI Sistémica en Administración Central.

Las OSI's en los recintos administran los DNS de sus respectivos recintos junto al bloque de direcciones IP asignados a éstos. Quienes deseen definir dominios adicionales para que ejecuten sobre la red del recinto deberán procurar la autorización para el mismo con la OSI del recinto.

ACCESO SEGURO A LA RED DE COMUNICACIÓN

La red universitaria conecta las redes de los recintos y múltiples dependencias, todas conectadas a una espina dorsal ("backbone") con dos rutas independientes. La mayor parte de las redes de los recintos son administradas por sus respectivas Oficinas de Sistemas de Información. Sin embargo, para departamentos con necesidades especializadas, se permite conectar redes locales no administradas por OSI.

Por lo general, una red no administrada por OSI es financiada, administrada o mantenida – incluyendo tareas como el cableado y conexión – en responsabilidad primaria de un departamento, colegio o facultad. Se debe destacar que aunque la red universitaria y las redes de los 11 recintos se clasifican por separado, las prácticas y procedimientos relevantes deben ser consistentes.

Para que funcionen de manera integrada, los componentes de la red deben tener un acuerdo implícito de confianza entre sí. Por lo tanto, toda la infraestructura de red – sea o no administrada por la OSI – deberá estar protegida al nivel más alto. Todo esfuerzo para conectarse a la red de un recinto debe coordinarse a través de la OSI de ese recinto. Todo esfuerzo para conectarse a la red sistémica deberá coordinarse a través de la OSI Sistémica en Administración Central, dado el impacto que tiene un cambio en la red de comunicaciones a nivel sistémico. Los administradores de la red protegerán la misma mediante la implantación de mecanismos de autenticación para validar el acceso legítimo de los usuarios.

Todo usuario y administrador que acceda la red universitaria debe asegurarse que ha tomado todas las medidas posibles para asegurar la computadora que utilice para conectarse local o remotamente a la red universitaria. Los recursos aplicativos a través de la red se suministrarán según las necesidades del usuario o administrador; pero salvaguardando dichos recursos contra ataques e intentos de acceso no autorizados. Este Estándar también aplica a las conexiones remotas que se hagan a la red universitaria para llevar a cabo trabajos en beneficio de la Universidad, incluyendo pero sin limitarse a, leer y remitir correos electrónicos o acceder a recursos de la Web. Toda implantación de acceso remoto en la Universidad está sujeta a la Política y este Estándar.

ACCESO SEGURO A LA RED INALÁMBRICA

La Universidad suministra redes inalámbricas (WLAN o LAWN, por sus siglas en inglés) para permitir conectividad móvil y flexible a las redes locales y al Internet. La Universidad fomenta que se suministre acceso inalámbrico a una red donde sea viable; por ejemplo, donde las facilidades técnicas estén disponibles y los requerimientos técnicos y de seguridad permitan su utilización. La implantación de acceso inalámbrico se coordinará a través de la OSI correspondiente; quien será responsable por configurar el WLAN de modo que la conexión sea segura; y que se garantice la integridad de las redes, sistemas, aplicaciones y datos mediante la implantación de técnicas de segmentación y autenticación.

PROTECCIÓN DE LOS DATOS PRIVADOS

La Universidad es responsable por mantener estándares de seguridad elevados en el cuidado de la información privada o confidencial, según lo exigen leyes federales y estatales. Los datos que le pertenecen a la Universidad y que se almacenan o acceden mediante computadoras u otros dispositivos electrónicos deben estar protegidos contra la pérdida intencional o accidental de su confidencialidad, integridad o disponibilidad independientemente de su ubicación: dentro o fuera de los predios universitarios.

Los datos se deben tratar de acuerdo a su naturaleza: confidencial, privada o pública. La Universidad tratará toda información legal y contractualmente protegida como confidencial y privada; sea esta información de naturaleza investigativa, clínica, educacional o administrativa. Además, la Universidad le exigirá a cualquier persona que requiera acceder esta información, sea o no usuario de tecnología informática de la Universidad, que cumpla con la Política IT y con estos Estándares.

Los usuarios y administradores tomarán las medidas que sean razonables para asegurar el equipo a través del cual información privada se accede. Los recintos, departamentos y unidades de la Universidad llevarán a cabo inspecciones periódicas de los sistemas de información bajo su control que contengan, utilicen o accedan información privada o confidencial.

ELIMINACIÓN SEGURA DE LOS DATOS

Los datos privados y programas instalados en computadoras y otros dispositivos electrónicos y medios de almacenaje representan un riesgo sustancial al momento de disponer o transferir el equipo. Este riesgo se debe atender previo a la transferencia o disposición del equipo, mediante la eliminación segura de estos datos y programas. Se deben eliminar los datos privados cuando la transferencia del equipo sea hacia un destino desconocido o hacia una persona u oficina que no está autorizada para acceder dicha información privada. El departamento o individuo directamente responsable por los datos privados en la computadora o dispositivo electrónico deberá asegurarse que los datos privados han sido removidos de forma segura, previo a disponer del equipo fuera de su control. Este departamento o persona tomará los pasos necesarios para erradicar los datos almacenados en los medios de almacenaje, de modo que los datos ya no se puedan recuperar. Según se necesite apoyo técnico adicional, el departamento o persona podrá solicitar apoyo de OSI para cumplir con esta responsabilidad.

COMPARTIR ARCHIVOS ELECTRÓNICOS

Los usuarios y administradores deberán coordinar a través de la OSI previo a instalar y utilizar programas para compartir archivos o Peer-to-Peer (P2P). Aunque el compartir información es una parte endémica de la filosofía de la Universidad de Puerto Rico, se debe llevar a cabo de forma que cumpla con las leyes federales y estatales aplicables, al igual que con la Política vigente, estos Estándares y los procedimientos relevantes. La Universidad no prohíbe de manera

explícita la instalación de programas para compartir archivos. Sin embargo, cuando un programa de este tipo se instala, tiene activada por defecto una funcionalidad para compartir archivos. Esto representa un riesgo serio de seguridad, pues permite la entrada de programas cuyo propósito es invadir la red. También expone la Universidad a posibles violaciones e infracciones a la propiedad intelectual; aunque no se esté consciente de ello.

DISEÑO DE LAS PÁGINAS WEB Y APLICACIONES DE INTERNET

La misión universitaria de instruir, investigar y brindar servicio aplica a todos los individuos, sin importar que tales personas tengan alguna limitación física. La Universidad fomentará que sus tecnologías y fuentes electrónicas de información, en particular las páginas Web y aplicaciones de Internet, cumplan con todas las leyes y reglamentaciones federales y estatales aplicables; que le permitan a las personas con limitaciones físicas tener acceso a - y utilizar - las aplicaciones e información en una manera comparable al acceso y uso por personas sin tales limitaciones.

Al igual que formas impresas de comunicación tales como el papel y material timbrado, o material promocional, las páginas Web y aplicaciones de Internet son un reflejo gráfico de la Universidad ante el mundo externo. La Universidad y/o sus Recintos podrán definir y publicar el diseño de un marco general (colores, encabezados y logos, entre otros criterios) para alinear tales páginas y aplicaciones a la imagen institucional deseada. Dentro de este marco, los artistas gráficos y programadores de páginas Web tendrán un espacio amplio para diseñar las páginas y aplicaciones. Los investigadores y personal docente quedan eximidos de cumplir con este requisito, por la naturaleza del trabajo que le rinden a la Universidad. Sin embargo, todas las aplicaciones de Internet incluirán algún enlace hacia su Recinto o unidad institucional en la parte superior de la página. Este exención no significa que no se seguirán las mejores prácticas para diseñar y desarrollar aplicaciones Web. Las páginas se deben diseñar para que carguen relativamente rápido; para el beneficio de aquellos usuarios que no cuentan con acceso a un ancho de banda amplio.

Como corporación pública, la Universidad debe ejercer cuidado al colocar anuncios en sus comunicaciones que puedan interpretarse como un endoso comercial o político a terceros. Como regla general, no se permiten los endosos comerciales o políticas en las páginas y aplicaciones Web de la UPR. Cualquier anuncio que se justifique en términos de sus beneficios para la Universidad se permitirá sólo mediante autorización escrita por parte del oficial autorizado de la Universidad, a nivel institucional o del recinto.

EDUCACIÓN EN LA UTILIZACIÓN CORRECTA DE LA TECNOLOGÍA

Las OSI's (Sistémica y en los recintos) fomentarán la utilización correcta de los recursos de tecnología informática, su cumplimiento con la Política, con estos Estándares y con los procedimientos subordinados; mediante mecanismos periódicos tales como seminarios, charlas, talleres, conferencias y comunicaciones electrónicas hacia los miembros de la comunidad universitaria. Estos esfuerzos se podrán coordinar a nivel sistémico o de cada recinto. Podrán

darse utilizando recursos de la Universidad o recursos externos.

REVISIÓN DE LOS ESTÁNDARES, GUÍAS Y PROCEDIMIENTOS

Periódicamente, se necesitarán revisar los Estándares y sus procedimientos subordinados para adaptarlos a las necesidades cambiantes de la Universidad. La revisión puede venir como resultado de algún cambio en una legislación o en los reglamentos, políticas y certificaciones de la Universidad. Se puede dar la revisión según se implanten nuevas tecnologías, o cuando surjan mejores formas de utilizar la tecnología existente o mejores formas de llevar a cabo los procesos institucionales.

La Vicepresidencia de Investigación y Tecnología trabajará en conjunto con la OSI Sistémica y las OSI's en los diferentes recintos para revisar estas prácticas y procedimientos; particularmente en aquellos asuntos referentes a la adopción, implantación, utilización, seguridad, privacidad y propiedad intelectual de tecnología informática. Todo cambio a los Estándares y procedimientos existentes, o inclusión de nuevos Estándares y procedimientos, deben ser cónsono con la Política IT y con estos Estándares.

DEFINICIONES

Las siguientes definiciones se proveen para la conveniencia del lector. Incluyen términos mencionados a través de este documento, los cuales son comunes en la industria de la informática.

- **ACCESO MEDIANTE UN PUERTO EN LA RED**

  Punto de acceso en una red de comunicación. Puede ser en la forma de una conexión por discado ("dial in"), una conexión alámbrica de topología Ethernet o una conexión inalámbrica. Se designan como puertos abiertos o puertos estándares.

- **ADWARE**

  Los programas de tipo "Adware" automáticamente ejecutan, despliegan o cargan material promocional a una computadora, una vez se haya instalado el programa o mientras se utilice el programa. En un contexto negativo, programas "Adware" maliciosos pueden tomar la forma de "spyware" (en la cual se rastrea, registra y vende información la actividad de un usuario o administrador, sin que estos lo sepan y sin su consentimiento) o "malware" (en el cual se interfiere con la función de otros programas legítimos a modo de obligar al usuario a visitar alguna página Web específica).

- **ANCHO DE BANDA**

  En las telecomunicaciones, el 'ancho de banda' es el término que hace referencia al método de señal que atiende una gama amplia de frecuencias divididas en canales. A mayor el ancho de banda, mayor la capacidad para transmitir información.

- **ANTI-SPYWARE**

  Programa especializado para proteger un servidor o computadora de los efectos de programas de tipo "spyware".

- **ANTI-VIRUS**

  Programa especializado para proteger un servidor, computadora, equipo de red, aplicación o datos de los efectos de virus, troyanos o gusanos.

- **CABALLO DE TROYA**

  Programa que contiene o instala código malicioso (conocido como "carga" o "troyano"). El programa puede ser un programa legítimo que haya sido infectado con el código para replicación.

- **DATOS PRIVADOS**

  El concepto "dato privado" se define como información de la Universidad que está legal o contractualmente protegida y que la Universidad viene obligada a tratar como confidencial y

privilegiada, sea información de naturaleza investigativa, clínica, educacional, social o administrativa. Algunos ejemplos de datos privados se presentan a continuación.

- Número de seguro social
- Propiedad intelectual
- Edad o fecha de nacimiento
- Dirección residencial
- Número de teléfono residencial
- Información sobre su salud
- Ubicación de activos
- Identificar el usuario con temas sobre los cuales tiene preferencia o sobre los que ha solicitado en el pasado
- Etnicidad
- Ciudadanía
- Número de pasaporte
- Condición de incapacidad
- Credo o preferencia religiosa o política
- Género
- Donantes anónimos
- Información personal del estudiante (la cual no debe ser divulgada, salvo bajo casos específicos)

Algunos ejemplos de información que no debe ser divulgada se presentan a continuación:

- Calificaciones académicas
- Cursos tomados
- Itinerarios
- Resultados de exámenes
- Registros sobre consejerías
- Servicios educativos recibidos
- Acciones disciplinarias

A continuación se presentan algunos ejemplos de información contractualmente protegida:

- Número de tarjeta de crédito
- Número de identificación personal (PIN, por sus siglas en inglés), utilizado para identificar usuarios en sistemas financieros

- **DNS O "DOMAIN NAME SYSTEM"**

  El Sistema Denominacional de Dominios ("Domain Name System" o DNS, por su término en inglés) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico bajo un dominio.

- **DOMINIO DE INTERNET**

  Un dominio de Internet es un nombre base que agrupa a un conjunto de equipos o dispositivos; y que permite proporcionar nombres de equipo que son más fáciles de recordar

que una dirección IP numérica. Al igual que la dirección IP, el dominio permite ubicar los equipos que se agrupan bajo éste. Como regla general, el nombre con el que se designa un dominio identifica la institución a la cual pertenece.

- **ELIMINACIÓN SEGURA DE DATOS**

  La eliminación segura de datos se refiere al proceso de erradicar los datos almacenados en medios electrónicos (disco duro, cinta magnética, CD, DVD, flash drive), de modo que estos datos ya no se puedan recuperar. Esto se logra de varias maneras: utilizar un programa especializado de eliminación segura para escribir caracteres aleatorios en múltiples pases sobre los datos; sustituyendo el contenido del disco duro con una imagen que no contiene datos privados; o destruyendo el disco duro. Medios electrónicos, tales como cintas magnéticas, CDs, u otros medios con datos privados, deben también someterse a eliminación segura o destruirse totalmente, previo a disponer de ellos.

- **EQUIPO ("HARDWARE")**

  Término genérico utilizado para referirse a los artefactos y dispositivos físicos de tecnología, tales como computadoras, impresoras o equipo de comunicación.

- **GUSANO**

  El gusano es un programa malicioso de computadoras que se replica de computadora en computadora. Utiliza la red de comunicación para remitir copias de sí a otros nodos de la red sin intervención de un usuario o de un administrador. Contrario a un virus, no requiere anejarse a un programa o archivo existente. Los gusanos siempre impactan adversamente la red de comunicación; aunque sea por su consume del ancho de banda; mientras que los virus se enfocan en corromper archivos de computadoras seleccionadas.

- **INTERNET PROTOCOL (IP)**

  Se conoce como protocolo de Internet (IP, por sus siglas en inglés) a las reglas estándares que rigen la sintaxis, semántica y sincronización para comunicar datos a través de redes de telecomunicación.

- **LAN**

  Red local de comunicación. Las siglas significan "Local Area Network".

- **LAWN**

  Local Area Wireless Network (también conocida como "WLAN").

- **MALICIOUS HACKING**

  El término "hacking" significa "cortar" en inglés. Alude a violentar la seguridad de un programa, sistema o aplicación de computadora, o de una red de comunicación, para lograr acceso ilegal a los recursos de la red de comunicación.

- **MEDIO DE ALMACENAJE**

  Cualquier dispositivo que se utilice para contener o acceder datos o archivos a través de una computadora. Puede ser fijo, como en el caso de los discos duros. También puede ser removible, como lo es un diskette, disco compacto (CD's), disco de video digital (DVD's), cartucho de cinta magnética o dispositivo "pen drive" (también conocido como dispositivo USB).

- **OFICINA DE SISTEMAS DE INFORMACIÓN (OSI)**

  La oficina específicamente autorizada por la Universidad para proteger los datos y recursos de tecnología de la información. La OSI sistémica está ubicada en Administración Central, mientras que cada recinto tiene una OSI local, aunque esté designada bajo otro nombre.

- **PROGRAMA ("SOFTWARE")**

  Los programas son componentes lógicos de instrucciones que rigen la operación de los equipos tecnológicos ("hardware") mediante funciones especializadas tales como el sistema operativo, las aplicaciones comerciales, sistemas de manejo de bases de datos o sistemas de correo electrónico.

- **PROGRAMAS MALICIOSOS (MALWARE)**

  Programas diseñados para infiltrar o averiar los sistemas, aplicaciones o datos en una computadora sin el consentimiento informado de su dueño. Abarca programas tales como virus, gusanos, caballos de troya, "spyware", programación "adware" ilícita y cualquier otro código malicio y no deseado. El término jurídico de este tipo de programa es el de contaminante de computadora. El malware puede haber sido instalado intencional o accidentalmente en una computadora.

- **PUERTO ABIERTO**

  Un puerto abierto en la red de comunicación puede ser utilizado por más de una computadora para accede a la red. Como mecanismo de proteger la red de comunicación, se requiere que la computadora se autentique, previo a permitir pasar su tráfico. Un puerto abierto debe estar sujeto a re-autenticaciones periódicas cada número predeterminado de horas, para mantener la seguridad de la red.

- **PUERTO ESTÁNDAR**

  Un puerto estándar en la red de comunicación tiene un solo equipo conectado permanentemente a él. Como regla general, es más seguro que un puerto abierto.

- **RED DE COMUNICACIÓN**

  Una red de computadoras conectadas mediante algún sistema de telecomunicaciones para transmitir información y compartir recursos. También se le conoce como red de

telecomunicación.

- **RED INALÁMBRICA**

  En una red de comunicación tradicional, las computadoras se conectan a la red mediante cables o "alambres". En contraste, una red inalámbrica provee esta conectividad mediante dispositivos que utilizan radio-frecuencia para habilitar este enlace entre las computadoras. La conexión inalámbrica también se conoce como acceso 'Wi-Fi' (del término "wide fidelity").

- **RED LOCAL DE COMUNICACIÓN**

  Red de comunicación que cubre un área geográfica relativamente pequeña; tal como el área cubierta por una oficina, recinto o grupo de edificios.

- **RED SISTÉMICA**

  Red de comunicación que interconecta las diferentes redes locales implantadas en Administración Central y en las diferentes unidades de la Universidad de Puerto Rico; y que a su vez conecta éstas con el Internet e Internet2.

- **SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)**

  Los programas IDS avisan contra intentos no autorizados de terceros desconocidos para acceder una computadora. IDS le permite al usuario o administrador conocer que alguien intenta violentar un sistema.

- **SPYWARE**

  Programa que recopila información personal acerca del usuario o administrador, sin su consentimiento. Su propósito varía desde lo abiertamente criminal (robo de contraseñas o datos financieros) hasta lo meramente inconveniente (registrar el historial de búsquedas por el Internet para promociones enfocadas, a la vez que consume recursos computacionales). Los programas de tipo spyware recopilan diferentes tipos de información. Algunos intenta rastrear los sitios visitados en el Internet para luego remitir esta información a compañías de publicidad. Otras variantes maliciosas intentan interceptor las contraseñas o los datos de tarjetas de crédito según el usuario teclea estos datos.

- **TECNOLOGÍA INFORMÁTICA O TECNOLOGÍA DE LA INFORMACIÓN**

  La tecnología informática abarca las disciplinas que estudian, diseñan, desarrollan, implantan, apoyan o mantienen aplicaciones de sistemas de información. Incluye los equipos, redes de comunicación, programas y datos que componen estas aplicaciones. IT atiende la utilización de estos equipos y programas para recopilar, almacenar, convertir, proteger, procesar, transmitir, recuperar e informar la información de manera segura y exacta.

- **VIOLACIÓN**

  Cualquier acción no permitida o contraria a la *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*, contraria a estos Estándares, o contraria a las Guías y Procedimientos que rigen el uso de tecnología a nivel sistémico o en las unidades.

- **VIRUS**

  Programa que se replica a sí mismo e infecta una computadora sin el consentimiento o conocimiento del usuario o administrador de la computadora. El virus original pudiera modificar sus copias; o éstas se pueden auto-modificar. Un virus sólo puede replicar de una computadora a otra cuando su portador se coloca en una computadora no infectada. Por ejemplo, un usuario o administrador pudiera transferirlo a través de la red de comunicación en un medio de almacenaje portátil tal como un diskette, disco compacto (CD) o dispositivo "pen drive". Un virus también se puede replicar viajando a través de la red de comunicación.

- **WAN**

  Red sistémica de comunicación. Las siglas significan "wide area network".

- **WLAN**

  Se refiere a una red inalámbrica. También se le conoce como "Wireless Local Area Network" o "Wireless LAN" o LAWN.

HISTORIAL DE REVISIONES

Revisión	Fecha	Descripción
0	4-Abr-2008	Emisión inicial de los ***Estándares para la Utilización Aceptable de Recursos Informáticos***, en acorde con la *Política Institucional para la Utilización Aceptable de los Recursos de la Tecnología de la Información en la Universidad de Puerto Rico*.

STANDARDS FOR THE ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

UNIVERSIDAD DE PUERTO RICO

Issued on April 4, 2008

Approved by:

Emma Fernández-Repollet, Ph.D.
Vice President for Research and Technology

4/7/08
Date

TABLE OF CONTENTS

INTRODUCTION TO USING INFORMATION TECHNOLOGY RESOURCES 1

REFERENCE SOURCES 1

ACQUIRING AND ADMINISTRATING IT RESOURCES 1

USING HARDWARE AND SOFTWARE RESOURCES 2

SECURING INFORMATION TECHNOLOGY RESOURCES 2

USING ID AND PASSWORD 3

ADMINISTRATING DOMAINS 3

SECURE ACCESS TO THE NETWORK 3

ACCESSING WIRELESS NETWORKS 4

SECURING PRIVATE DATA 4

SECURELY DELETING DATA 5

FILE SHARING THROUGH PEER-TO-PEER (P2P) PROGRAMS 5

DESIGNING WEB SITES AND WEB APPLICATIONS 5

EDUCATING FOR THE CORRECT USE OF TECHNOLOGY 6

MAINTAINING IT STANDARDS & PROCEDURES 6

DEFINITIONS 8

REVIEW HISTORY 13

INTRODUCTION TO USING INFORMATION TECHNOLOGY RESOURCES

The information within this document is subordinate and subject to the Board of Trustee's Certification # 35, 2007-2008 Series: the *System-Wide Policy for the Acceptable Use of Information Technology Resources Throughout the University of Puerto Rico* (henceforth, the "IT Policy"). The standards contained herein must be adhered to by all users and technology administrators. Compliance with these Standards ensures compliance with the IT Policy; and enables the best possible use of the IT resources available to the University of Puerto Rico.

All IT procedures as well as campus IT policies throughout the University must be aligned with the IT Policy as well as with these Standards. Final interpretation of the meaning, intent, and approach towards their application lies within the exclusive domain of the Vice President for Research & Technology.

REFERENCE SOURCES

Several sources of information have been used as input for this document, to guarantee comprehensiveness. They include existing policies and guidelines from other universities both within and outside the U.S., applicable federal and Commonwealth legislation, best practices from recognized industry authorities and experts, and other peer reviewed sources.

ACQUIRING AND ADMINISTRATING IT RESOURCES

The ISO will identify the minimum hardware and software specifications for acquiring information technology equipment and software. ISO will make these specifications available to the general university population. Users and technology administrators will use these specifications when requisitioning computers and software. However, University researchers may choose to follow these specifications or not depending on their specialized needs, due to the specialized nature of their institutional work.

Acquisition and installation of hardware and software (including operating systems) for which ISO support is expected and required must be coordinated through the ISO; that ISO may confirm its ability to support this hardware and software.

Industry guidelines establish a technology's useful life in terms of the number of years it may be productively used by an institution. All campuses, departments, and offices should consider the useful life of their information technology equipment during the reviews of their respective annual budgets and plan accordingly for the timely substitution of their computers and devices when they reach the end of their useful life; provided that adequate funding is available. In this endeavor, ISO may provide assistance to identify particular equipment model's age, technical specifications, and estimated replacement cost.

The ultimate determinants as to how long information technology equipment lasts are the care and preventive maintenance provided to it and the support available from the technology

industry. The decision to acquire new technology rather than repair existing technology should be based on which is the lesser cost. Acquisition of new equipment, rather than repairing the existing equipment should be authorized by the office or laboratory director.

All information technology equipment and software purchased through the University is considered the sole property of the University. Acquisitions of Information Technology equipment will be done in compliance with the IT Policy and the Board of Trustee's Certificate # 62, Series 1994-1995, *Regulation for Control of Fixed Assets in the University of Puerto Rico*.

Software acquisitions will be acquired in compliance with the IT Policy. Non-standard software will be acquired following the IT Policy and the applicable regulations and procedures regarding the acquisition of non-personal equipment, supplies, and services at the University of Puerto Rico.

In order to make the best possible use of available technology resources, offices, campuses, and faculties may transfer productive equipments following appropriate control procedures. Damaged equipment may be repaired as long as it is economically feasible for the University. Otherwise, it will be disposed in compliance with the applicable regulations regarding the control of fixed assets in the University of Puerto Rico.

USING HARDWARE AND SOFTWARE RESOURCES

University computers, networks, systems, applications and data are to be used only for legitimate, authorized purposes. User and technology administrators will utilize only the hardware and software legally made available to them. No user and technology administrator must ever engage in, promote, cause, abet, or allow any activity that might be harmful to any University equipment, network, system, application or data; since this would inhibit other user and technology administrators from conducting their own legitimate work for the University.

Avoid unapproved changes to a computer's configuration, as this may hamper the computer´s connectivity to network services.

A user and technology administrator should either lock or logoff from a computer being used whenever he or she steps away; to avoid unauthorized use of his or her work session.

SECURING INFORMATION TECHNOLOGY RESOURCES

In an endeavor to secure University IT resources, user and technology administrators should take all reasonable precautions to protect University computers (including servers), networks, applications, and data. Such measures should include special arrangements for housing the IT equipment (temperature and humidity control, physically controlled access, fire suppression, etc.) in line with the equipment's criticality; as well as using specialized hardware and software to protect these IT resources and the data contained therein. Third parties who connect their equipment to the University network must also provide similar protection for their computers.

Malicious software represents a substantial risk to the University community in terms of time, money, and potential loss of computer software and/or data. As part of the endeavor to secure and protect all equipment that accesses University data, every computer and server connected to the University network is required to maintain and use up-to-date versions of protective software such as anti-virus, anti-spyware, or intrusion detection software configured according to relevant IT system-wide procedures. User and ISO's will regularly apply vendor-issued critical security updates and patches to installed software to protect University computers (including servers), networks, systems, applications, and data. Administrators of servers and network equipment will take steps to apply security and firmware updates with minimal to no impact or interruption to system availability by users.

Furthermore, University users and technology administrators should periodically backup critical applications and data to allow continuity in the event of emergencies.

USING ID AND PASSWORD

The combination of username (user ID) and password is uniquely assigned to each user and technology administrator as a mechanism to ensure that only an authorized person may access University data and systems over the network. User and technology administrators will take the necessary steps to protect these, whether accessing systems locally or remotely, in compliance with the IT Policy, these Standards, and subordinate system-wide procedures implemented throughout the University. Strong passwords should be used to minimize the probability of unauthorized access, following the techniques identified within *ISO Security Norms*.

ADMINISTRATING DOMAINS

The University and its Campuses have established a virtual presence over the Internet through the use of domains. The System ISO administers and operates the University DNS UPR.EDU and the Internet Protocol (IP) address space assigned to them. Anyone wishing to define additional domains to run on the University network or represent the University must coordinate and obtain approval from the System ISO.

Each Campus ISO administers and operates the Internet domain for their respective Campuses and the IP address space assigned to them. Anyone wishing to define additional domains to run on the Campus network or represent the Campus must coordinate and obtain approval from the Campus ISO.

SECURE ACCESS TO THE NETWORK

The University network consists of Campus Area Networks and many dependencies all connected to a high-speed, broadband backbone. The majority of the campus networks are run centrally by campus ISO but for those departments with certain specialized needs, non-ISO local networks are allowed to connect to the campus backbone network.

As a general rule, a non-ISO network is financed, administered, and maintained primarily by a department, faculty or facility. Nevertheless, although said network may be seen as a separate resource, relevant practices and procedures should be consistent with the IT Policy and these Standards.

To function, the elements of the network must have an implicit trust arrangement with each other. Thus, the entire network infrastructure (i.e. network equipment such as routers and switches), whether on ISO or non-ISO networks, must be secured to a high level. All efforts to connect to the campus network must be coordinated through the Campus ISO. Efforts to connect to the university network must be coordinated through the System ISO, given the system-wide impact that any change here may have. Furthermore, network administrators shall protect the network by implementing authentication to validate the legitimate access of authorized users.

Every user and technology administrator of University IT resources must make sure that all possible measures have been taken to secure the computers used to connect, whether locally or remotely, turned on or off, to the University network. Application resources over the network shall be provided, based upon user and technology administrator needs, but will be subject to protecting said resources against attacks and unauthorized access attempts. This Standard applies to remote access connections used to do work on behalf of the University, including but not limited to, reading or sending e-mail and viewing intranet Web resources. All remote access implementations at the University are covered by the IT Policy and this Standard.

ACCESSING WIRELESS NETWORKS

The University provides wireless networks (also called wireless local area networks, WLAN's or LAWN's) to allow flexible, mobile connectivity to the Campus and University networks, and the Internet. Wireless access should be implemented wherever feasible: i.e., wherever technical facilities are available and the applications' security and technical requirements permit their use. University administrators wishing to implement wireless access and user wishing to access WLAN's should coordinate the effort through the System or Campus ISO. System and Campus ISO are responsible for configuring the WLAN to guarantee secure access to Campus and University networks, applications, and data by implementing segmentation and authentication.

SECURING PRIVATE DATA

The University is responsible for maintaining high standards of security for private/non-public electronic information, as required by federal and Commonwealth laws. University data that is stored on or accessed by computers or other electronic devices must be secured against intentional or accidental loss of confidentiality, integrity, or availability regardless of location: whether on campus or off campus.

Information should be treated in accordance with its nature: confidential, private, or public. The University will treat all legally and contractually protected non-public University data as

confidential; whether it is research, clinical, educational, outreach, or administrative data. Furthermore, the University will hold any person who requires access to University information, whether or not said person is a user and technology administrator of University Information Technology, to comply with the IT Policy and these Standards.

User and technology administrators will take reasonable steps to secure all hardware through which private data may be accessed. University offices, campuses, faculties, and units shall conduct periodic reviews of information systems under their control that contain private or confidential data.

SECURELY DELETING DATA

Non-public data and licensed software remaining on computers, other electronic devices, and storage media at the time of transfer or disposal represent a substantial security risk that should be addressed through secure data deletion. Non-public information must be securely deleted from any and all devices which will be disposed of or transferred from a current User and technology administrator to an unknown destination or to another User and technology administrator who is not authorized to the data. The department or individual directly responsible for non-public data on a University computer or other electronic device is required to ensure that any non-public information on that device is securely removed before disposing of the device beyond their direct control. The department or individual directly responsible for non-public data on a University computer or other electronic device shall take the required steps to eradicate data contained on any form of electronic storage media in a manner that makes it totally impossible to recover the data, before said electronic storage media is transferred or otherwise disposed of. If necessary, said department or individual may request assistance from ISO to comply with this responsibility.

FILE SHARING THROUGH PEER-TO-PEER (P2P) PROGRAMS

User and technology administrators should coordinate with ISO before installing and using file sharing or peer-to-peer (P2P) programs. Although information sharing is an integral part of the University's philosophy, it should be done in a manner that complies with the IT Policy, these Standards, and relevant Procedures. The University does not explicitly prohibit the installation of these programs. Nevertheless, when a program of this type is installed, its file sharing functionality is activated by default. This is a serious security risk, since it represents a way in for programs whose intent is to exploit network vulnerabilities. Also, users and technology administrators open themselves – and the University – to possible violations and infringements of copyright law, even without their knowledge.

DESIGNING WEB SITES AND WEB APPLICATIONS

The University's mission of instruction, research, and service outreach applies to all individuals, regardless of whether an individual has a physical limitation. The University will promote that its

technologies and electronic sources of information, particularly web pages and web sites, comply with applicable federal and Commonwealth legislation and regulations; to allow individuals with disabilities have access to and use information and data in a manner that is comparable to that by individuals without disabilities.

As with written communication forms such as University stationary and promotional material, University web pages and web sites reflect a graphical image of the University to the outside world. The University and/or its Campuses may define and publish basic design frameworks (colors, headings, and logos, among other criteria) to align their web pages and sites with a desired institutional image. Within a framework, individual designers have ample leeway for designing web pages and applications. University researchers and academicians are exempt from having to comply with these frameworks, due to the specialized nature of their institutional work. Nevertheless, all web sites will include, as a minimum, a link to their Campus or institutional unit on the site's top page. This exemption does not preclude from the use of best practices for website design or application development. All web sites on the UPR domain must comply with UPR's legal and policy guidelines. Web pages should be designed to load fairly quickly; for the benefit of those users who do not have broadband access.

As a public corporation, the University must exercise care when placing notices on any form of communication which may be construed as an advertisement or endorsement of any external commercial or political entity. As a general rule, political or commercial advertisements in UPR websites are not allowed. Any advertisement through UPR websites that is justified in terms of its benefits to the University may be allowed after written approval from the corresponding University official – the President, the chancellors, or their designated representative - at the Institution or Campus level.

EDUCATING FOR THE CORRECT USE OF TECHNOLOGY

System and Campus ISO will promote the correct use of IT resources and compliance with the IT Policy, these Standards, and the applicable subordinate procedures, through a permanent campaign using such mechanisms as periodic seminars, workshops, conferences, and written and electronic forms of communications issued to the user and technology administrator communities throughout the University. This effort may be coordinated and conducted at the campus level as well as through Central Administration; and may be conducted using either University or non-University resources.

MAINTAINING IT STANDARDS & PROCEDURES

From time to time, it may be necessary to review these Standards, and their subordinate procedures, to adapt them to the University's changing needs. Said review may be required as a result of changes in legislation or University regulations, policies, and bylaws. Reviews may also be required to address emerging technologies, better ways to use current technologies, better ways to execute processes, or whenever new technology is implemented.

The Vice President for Research & Technology will work with the System and Campus ISO's to review these Standards and Procedures; in particular where issues of information technology adoption, use, security, privacy, and intellectual property are concerned. Any change to existing Standards and Procedures – as well as the incorporation of any new Standard or Procedure – must be consonant with the IT Policy and these Standards.

DEFINITIONS

The following definitions are provided as a convenience for the reader. The definitions include terms referred to throughout this document, which are endemic to the information technology industry.

- **ADWARE**

  Advertising-supported software (Adware) is software that automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while an application is being used. In a negative context, malicious adware may take the form of spyware (in which information about the user and technology administrator's activity is tracked, reported, and often re-sold, without the user and technology administrator's knowledge or consent) or malware, which may interfere with the function of other software applications, in order to force user and technology administrators to visit a particular web site.

- **ANTI-SPYWARE**

  Specialized software used to protect a server or user and technology administrator computer from the effects of spyware.

- **ANTI-VIRUS**

  Specialized software used to protect a server, user and technology administrator computer, network systems, applications, and data from malware such as viruses, Trojan horses, or worms.

- **BROADBAND**

  In telecommunications, broadband is a term which refers to a signaling method which handles a wide (broad) range of frequencies divided into channels. The wider the bandwidth, greater is the information carrying capacity.

- **DOMAIN NAME SYSTEM (DNS)**

  The Domain Name System is a distributed hierarchical database that stores information associated with Internet Domain names. Common uses include designating domain names to IP addresses and locating e-Mail servers under a designated domain.

- **HARDWARE**

  General term used to refer to physical artifacts of technology, such as computers or communications routers.

- **INTRUSION DETECTION SOFTWARE (IDS)**

  IDS alert computers to unknown, unauthorized access attempts. IDS let user and technology

administrators know that someone or something is trying to get into the system.

- **INFORMATION SYSTEMS OFFICE (ISO)**

  The office specifically empowered by the University with authority to protect information technology resources and data. The System ISO is located at the Central Administration, while each campus has its own Campus ISO, albeit under a different name.

- **INFORMATION TECHNOLOGY (IT)**

  Information Technology encompasses the study, design, development, implementation, support or management of computer-based information systems. IT includes computer hardware, network hardware, software applications, and data. IT deals with the use of hardware and software to store, convert, protect, process, transmit, retrieve, and report information, securely.

- **INTERNET DOMAIN**

  An Internet Domain is a base name that groups clusters of hardware devices. It allows designating names to identify this equipment which are easier to remember than numerical IP addresses. As with IP addresses, the Internet Domain identifies the equipment located within. As a general rule, the domain name identifies the institution to which it belongs.

- **INTERNET PROTOCOL (IP)**

  IP constitute the standard rules governing the syntax, semantics, and synchronization for communicating data across telecommunications networks.

- **LAWN**

  Local Area Wireless Network (also referred to as WLAN).

- **LOCAL AREA NETWORK (LAN)**

  A local area network is a computer network covering a small geographic area, such as an office, campus or a group of buildings.

- **MALICIOUS HACKING**

  Hacking refers to the modification of computer programs, systems or network security to exploit perceived weaknesses or achieve illegitimate access to IT or network resources.

- **MALICIOUS SOFTWARE (MALWARE)**

  Software designed to infiltrate or damage a computer's systems, application, or data without the owner's informed consent. It encompasses such programs as computer viruses, worms, Trojan horses, spyware, dishonest adware, and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant. Malware may have been purposely or accidentally installed on computers.

- **TELECOMMUNICATION NETWORK**

  A computer network is multiple computers connected together using a telecommunication system for the purpose of communicating and sharing resources.

- **NETWORK PORT ACCESS**

  A port refers to an access point into the network. It may range from a dial-in connection, to Ethernet connections, to a Wi-Fi (wireless) connection. Ports are designated as either standard or open.

- **OPEN PORT**

  An open port is a network port that may be used by more than one computer to connect to a network. Authentication is required on an open port before allowing traffic to pass, as a way to protect the network. Furthermore, an open port should be subject to re-authentication every pre-determined number of hours, for security purposes.

- **PRIVATE DATA**

  The term "private data" refers to legally or contractually protected non-public institutional data or data which the University is obliged to treat as confidential whether it is research, clinical, educational, outreach, or administrative data. Some examples of private/non-public data are:

  - Social security number
  - Ethnicity
  - Birth date
  - Linking library user and technology administrators with subjects about which information was requested
  - Citizen visa code or passport number
  - Citizenship
  - Trade secrets or intellectual property
  - Non-directory Student Information (not to be released except under prescribed conditions)

  Examples of non-releasable information include:

  - Grades
  - Courses taken
  - Schedule
  - Test scores
  - Advising records
  - Educational services received
  - Disciplinary actions

  Examples of contractually protected information:

  - Credit card numbers
  - Personal Identification Number (PIN)

- **SECURE DATA DELETION**

  Secure data deletion refers to a process of eradicating data on any electronic storage media in a manner that makes it totally impossible to recover the data. Secure deletion is achieved by an electronic wipe through a secure data deletion program for computers that writes random data in multiple passes; by replacing the current contents of a computer hard disk en masse with a base image of the computer disk (e.g. an image of the initial disk configuration, before the data was generated or stored on the disk); or by utterly destroying the physical media. Non-public information located on any storage media must be securely deleted or destroyed before disposing of the storage media beyond the custodian's direct control.

- **SOFTWARE**

  In contrast to hardware, software is the general term used to refer to the logical components of technology, such as the operating system, computer programs and the data accessed and maintained by the programs.

- **SPYWARE**

  Spyware is computer software that collects personal information about user and technology administrators without their informed consent. Purposes range from overtly criminal (theft of passwords and financial details) to the merely annoying (recording Internet search history for targeted advertising, while consuming computer resources). Spyware may collect different types of information. Some variants attempt to track the websites a user and technology administrator visits and then send this information to an advertising agency. More malicious variants attempt to intercept passwords or credit card numbers as a user and technology administrator enters them into a web form or other applications.

- **STANDARD PORT**

  A standard port is a network port that has a single machine continuously connected to it. It is generally more secure than an open port.

- **STORAGE MEDIA**

  Any device used to store or retrieve data or application files from a computer. Storage media may be fixed, such as a hard disk; or removable, such as floppy diskettes, magnetic tape cartridges, compact disks (CD's), digital video disks (DVD's), or pen drives (also known as USB drives).

- **TROJAN HORSE**

  A Trojan horse is a program that contains or installs a malicious program (sometimes called the payload or 'Trojan'). The program may be a legitimate program that has been hacked to insert malicious code.

- **VIOLATION**

  Any action contrary to the Acceptable Use IT Policy, these Standards, or the subordinate IT policies and procedures is considered a violation.

- **VIRUS**

  A virus is computer program that copies itself and infects a computer without permission or knowledge of the user and technology administrator. The original may modify the copies or the copies may modify themselves. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user and technology administrator sending it over a network or carrying it on a removable storage medium such as a diskette, CD, or pen drive. Viruses can also spread to other computers by infecting files over a network.

- **WIDE AREA NETWORK (WAN)**

  System-wide communications network that interconnects the different local area networks (LAN's); and also connects these local area networks to the commodity Internet and Internet2.

- **WIRELESS NETWORK**

  In traditional networks, computers are connected to telecommunications equipment via cables or 'wires'. As opposed to 'wired' networks, a wireless network provides this link through devices that use radio frequency to achieve the same link between computers. Wireless access is also known as 'Wi-Fi' (for wide fidelity) access.

- **WLAN**

  Wireless Local Area Network or Wireless LAN (also referred to as LAWN).

- **WORM**

  A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user and technology administrator intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

REVIEW HISTORY

Version	Date	Description
0	4-Abr-2008	Initial version of the ***Standards for the Acceptable Use of IT Resources***, in line with the *System-Wide Policy for the Acceptable Use of Information Technology Resources Throughout the University of Puerto Rico.*