Intertek

Política Corporativa de Uso Aceptable de la Tecnología (AUT)

Clasificación de datos:
Protegido

Version:
3.8

Autor del documento:
Intertek Global Cyber Security Team

Última actualización:
Enero-2024

Tabla de contenido

1. PROPÓSITO

El propósito de esta política es establecer el uso aceptable del equipo o tecnología de Intertek (computadoras, dispositivos móviles, redes, etc.) y establecer reglas y directrices para prevenir el uso inapropiado que exponga a Intertek a riesgos, incluyendo la pérdida de información confidencial y de propiedad, pérdida de ingresos, compromiso de servicios comerciales y posibles reclamaciones legales y regulatorias.

La seguridad efectiva del sistema es un esfuerzo en equipo que involucra la participación y el apoyo de cada Usuario de Intertek. Es responsabilidad de todos los Usuarios conocer estas directrices y actuar en consecuencia.

La Política de Uso Aceptable no constituye un contrato de empleo ni una promesa de empleo por un período definido. Esta política no altera la naturaleza discrecional del empleo de ningún empleado con Intertek.

2. ALCANCE DE LA POLÍTICA

GENERAL: Esta política se aplica a todos los empleados, contratistas, consultores, trabajadores temporales o terceros y trabajadores o "Usuarios" que trabajen en nombre de Intertek y tengan acceso a las tecnologías, equipos, dispositivos y otros recursos de la empresa, independientemente de su forma, ya sea física, lógica o digital. La política puede ser revisada en cualquier momento, con o sin previo aviso. Todos los Usuarios son responsables de leer y cumplir con esta política y cualquier revisión publicada que se le realice.

ESPECÍFICO DE LA POLÍTICA:

Aplicabilidad a Grupos y Entidades: La Política de Uso Aceptable de Tecnología de TI Corporativa ("UAP" o "Política") se aplica a INTERTEK GROUP PLC y sus entidades consolidadas ("Intertek").

3. MONITOREO Y ASEGURAMIENTO DEL CUMPLIMIENTO

NOTA: Las disposiciones de esta política están sujetas a las leyes y regulaciones locales aplicables que tienen precedencia.

Es responsabilidad de todos los gerentes de líneas de negocio, operaciones y TI asegurarse de que operan en conformidad con esta política.

El Equipo Global de Ciberseguridad llevará a cabo un proceso de revisión periódica para evaluar el cumplimiento a nivel global. Proveedores de aseguramiento independientes, como la Auditoría Interna del Grupo (por ejemplo, Auditorías Internas, Revisiones de los CMCs-Core Mandatory Controls), socios de auditoría externa o nuestros clientes, también pueden medir el cumplimiento a través de sus respectivas actividades de aseguramiento.

APLICACIÓN**:** Cualquier empleado que se determine haya violado esta política puede estar sujeto a acciones disciplinarias, hasta e incluyendo la terminación del empleo. Cualquier contratista que se determine haya violado esta política puede tener su contrato terminado.

4. EXCEPCIONES A LA POLÍTICA

Si una región, línea de negocio, aplicación, proyecto o cualquier otra función de Intertek no puede cumplir plenamente con alguno de los requisitos establecidos en esta política, se requiere una excepción formal y aprobada.

Las excepciones solo pueden solicitarse con base en un caso de negocio legítimo y deben documentarse y aprobarse, junto con una evaluación formal de riesgos, según el proceso especificado gestionado por el Equipo Global de Ciberseguridad.

Las excepciones se registran en un repositorio central y deben ser revisadas y re-aprobadas anualmente, o según lo requieran los cambios situacionales. Todas las excepciones se reportarán trimestralmente al Comité de Riesgos de TI del Grupo.

5. CICLO DE VIDA DE LA POLÍTICA

La política y los documentos asociados serán revisados anualmente, o según lo requieran los cambios situacionales, por el Equipo Global de Ciberseguridad. Estas revisiones podrían resultar en nuevas políticas, estándares o controles, y las actualizaciones podrían eliminar o aclarar las políticas, estándares o controles actuales. Las desviaciones de este proceso requerirán la aprobación del Jefe de Ciber GRC y serán reportadas al Comité de Riesgos de TI del Grupo y a la Alta Dirección, según sea necesario.

Las nuevas publicaciones o revisiones de la política serán aprobadas finalmente por el Comité de Riesgos de TI del Grupo.

6. ASISTENCIA Y ASESORAMIENTO

Para obtener asistencia y asesoramiento detallados sobre políticas, estándares y controles de TI, comuníquese con su representante local del Equipo Global de Ciberseguridad, o en casos donde se necesite mayor experiencia, envíe un correo electrónico a cyber.services@intertek.com.

7. ROLES Y RESPONSABILIDADES

1. El Equipo de Ciberseguridad Global es responsable de mantener y actualizar esta política.
2. El Equipo de Ciberseguridad Global es responsable de garantizar que las secciones generales de la política, así como las de seguridad e información propietaria, sigan siendo aplicables.
3. Legal, riesgos y cumplimiento son responsables de asegurar que las secciones de Internet, correo electrónico y comunicaciones sigan siendo aplicables.
4. Recursos Humanos es responsable de garantizar el reconocimiento de la política por parte de los empleados.
5. Es responsabilidad de cada empleado cumplir con esta política.

8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIONES DETALLADAS DE LA POLÍTICA		CMC/CISP LINK
8.1 POLÍTICAS GENERALES Los Usuarios deben seguir todas las políticas de Intertek al utilizar los recursos de Intertek, tales como tecnología de cómputo (hardware y software), móvil o de red. El cumplimiento de esta política complementa el Código de Ética de Intertek y sus políticas. Los Usuarios son responsables al usar los recursos de Intertek y deben asegurarse de que el uso sea apropiado y esté alineado con su rol y responsabilidades laborales. La Política de Uso Aceptable de TI debe ser comunicada a todos los empleados al momento de su contratación y durante su empleo, así como a otros Usuarios al inicio de su compromiso y durante el período en que proporcionen servicios a Intertek. Los programas continuos de capacitación y concientización refuerzan los requisitos de la política. Inicialmente, los Usuarios deben firmar o aceptar un Formulario de Política Aceptable al inicio del empleo y cada vez que se les otorgue acceso a recursos críticos de la empresa.		
AUT1	**Propiedad Intelectual** Intertek posee los Derechos de Propiedad Intelectual sobre todo el software, materiales y procedimientos desarrollados durante el tiempo de la empresa o utilizando los sistemas, redes o equipos de Intertek. Los Usuarios deben ser conscientes de que cualquier producto que creen, en cualquier forma, incluso después de su empleo en Intertek, seguirá siendo propiedad de Intertek. Toda la información transmitida, recibida o almacenada en las redes o dispositivos de Intertek, en cualquier tipo de medio de almacenamiento, ya sea físico o de software, será propiedad de Intertek o de los clientes de Intertek. La eliminación de dispositivos que contengan datos, incluidas computadoras personales y otros medios de almacenamiento, debe realizarse con métodos que aseguren la eliminación o destrucción de los datos.	**CDRP7**
AUT2	**Uso Personal** El uso personal breve y ocasional es aceptable siempre que no sea excesivo, inapropiado y no viole ninguna de las prohibiciones enumeradas en esta política, ni resulte en gastos para Intertek. Intertek se reserva el derecho de monitorear, limitar o suspender el uso personal a su absoluta discreción o si determina que un Usuario ha abusado de esta política. Los empleados de Intertek no tienen una expectativa razonable de privacidad sobre su uso de los recursos de Intertek, a menos que así lo exija la ley. Aunque los dispositivos personales, como los teléfonos móviles, pueden usarse para acceder a la red y servicios de Intertek, esta política no permite al Usuario utilizar los recursos de Intertek para uso personal. En consecuencia, el software comprado o aprobado por la empresa puede instalarse en equipos personales si la licencia específica del software permite el beneficio operativo del negocio, pero debe ir acompañado del permiso expreso de la alta dirección. Dicho software debe ser eliminado una vez que	**CDRP7**

	finalice el empleo o ya no esté en uso, o si hay un cambio en el rol y las responsabilidades laborales. Consulte la Política Corporativa BYOD de Intertek en la página de IT en la Intranet para obtener más requisitos con respecto al uso de dispositivos personales en el entorno de Intertek.	
AUT3	**Monitoreo de Red y Sistema** Individuos autorizados pueden monitorear los sistemas, equipos y tráfico de red de Intertek en cualquier momento. Intertek se reserva el derecho de monitorear, revisar y gestionar la información almacenada en los Activos y Recursos Tecnológicos de Intertek, de acuerdo con las leyes, regulaciones y políticas y procedimientos aplicables de Intertek. El monitoreo de Red y Sistema debe realizarse considerando la confidencialidad de la información.	**CDRP7**
8.2 SEGURIDAD Y PROPIEDAD DE LA INFORMACIÓN		
AUT4	**Clasificación de la Información** Consulte la Política de Clasificación de Datos de Intertek para obtener orientación sobre la clasificación de la información y las técnicas adecuadas de manejo de datos. Se debe observar la debida diligencia al manejar la información de Intertek. Esta información incluye datos de clientes, proveedores o terceros que están sujetos a cualquier norma legal, de cumplimiento y/o regulatoria. Ejemplos de dicha información suelen incluir código fuente, información privada de la empresa, estrategias corporativas, datos sensibles de la competencia, secretos comerciales, especificaciones, listas de clientes, información confidencial de clientes y datos de investigación. Los Usuarios deben tomar todas las medidas necesarias para evitar el acceso no autorizado a esta información. Todos los datos críticos almacenados en computadoras personales u otros dispositivos deben ser respaldados en los entornos corporativos de Intertek mediante métodos aprobados.	**CDRP7**
AUT5	**Configuración de Contraseñas** Los Usuarios deben mantener sus contraseñas seguras y no compartir sus cuentas. Los Usuarios son responsables de la seguridad de sus contraseñas y cuentas. Las contraseñas a nivel de sistema y de usuario deben cambiarse de acuerdo con la Política de Contraseñas de Intertek, y los Usuarios serán automáticamente notificados por Microsoft Active Directory para realizar estas actualizaciones.	**CDRP7**
AUT6	**Configuración de Bloqueo de Computadoras**	**CDRP7**

	Todas las estaciones de trabajo y otros dispositivos deben estar protegidos con un protector de pantalla con contraseña que tenga la función de activación automática configurada según lo establecido en el documento de la política de directrices de contraseñas, o cerrando la sesión (control-alt-delete) cuando la estación de trabajo o el dispositivo esté desatendido.	
AUT7	**Software de Protección de Puntos de Extremo de Seguridad** Todos los portátiles, PC, dispositivos móviles, etc., que estén conectados a las redes de Intertek, ya sean propiedad del Usuario o de Intertek, deben tener instalado un software de protección de seguridad aprobado y aceptado por el departamento de TI (antivirus, anti-spyware/malware, cortafuegos, etc.).	**CDRP7**
AUT8	Los derechos de administración para los dispositivos de Intertek solo deben ser gestionados por individuos específicos dentro del departamento de TI del Grupo Intertek.	**CDRP7**
8.3 ACTIVIDADES DE INTERNET, CORREO ELECTRÓNICO Y COMUNICACIÓN		
AUT9	**Uso Aprobado por la Administración** Intertek proporciona acceso a correo electrónico e Internet para ayudar a los Usuarios en el trabajo que realizan para o en nombre de Intertek. Aunque el uso de Internet y correo electrónico está destinado a actividades relacionadas con el negocio, el uso personal breve y ocasional es aceptable siempre que no sea excesivo ni inapropiado, no viole ninguna de las prohibiciones enumeradas a continuación y no resulte en gastos para Intertek. La administración se reserva el derecho exclusivo de determinar si algún uso es inapropiado, excesivo o viola esta política. Todo el equipo y las redes proporcionados por Intertek son propiedad de Intertek y, como tal, a menos que esté prohibido por la ley, no existe una expectativa razonable de privacidad en relación con el uso de este equipo. Intertek se reserva el derecho de monitorear, limitar o suspender el uso personal de sus sistemas, equipos y redes a su absoluta discreción.	**CDRP7**
AUT10	**Instalación de Software** No se debe instalar ningún software en los activos de Intertek o en dispositivos personales a menos que esté aprobado por la gerencia, debidamente licenciado y evaluado y aprobado por Ciberseguridad.	**CDRP7**
AUT11	**Información de Intertek** Los usuarios pueden encontrar información adversa o negativa en Internet relacionada con Intertek o sus servicios. Si se encuentra dicha información, los usuarios no deben responder, sino que deben informar a la Gerencia, quien determinará si es apropiado responder a la información.	**CDRP7**
AUT12	**Acoso / Contenido Inaceptable** La información utilizada o accedida por los usuarios a través de los sistemas, equipos o redes de Intertek no debe contener material que pueda considerarse ofensivo, abusivo, pornográfico, obsceno, profano, discriminatorio, acosador, insultante, denigrante,	**CDRP7**

	inflamatorio, fraudulento o de cualquier otra forma ilegal. El contenido inaceptable puede incluir, entre otros, comentarios o imágenes sexuales, insultos raciales, comentarios específicos de género o cualquier otro comentario o imagen que pueda ofender razonablemente a alguien por motivos de raza, edad, sexo, religión, color, origen nacional, discapacidad o cualquier otra base protegida por la ley. Utilizar los sistemas, equipos o redes de Intertek para participar en cualquier forma de acoso, ya sea por correo electrónico, teléfono, buscapersonas, o mediante el lenguaje o la frecuencia o tamaño de los mensajes, está prohibido. Cualquier violación someterá al usuario a acciones disciplinarias, incluidas el despido o la terminación de su contrato.	
AUT13	**Actividades Prohibidas en Internet, Correo Electrónico y Comunicaciones** Los usuarios no deben: • Transmitir, reenviar, transmitir o descargar material que sea ofensivo, abusivo, explícitamente sexual, imágenes violentas, pornográficas, obscenas, profanas, discriminatorias, acosadoras, insultantes, denigrantes, inflamatorias, fraudulentas, que consuman ancho de banda y/o afecten la productividad general del sitio o que sean ilegales. Los usuarios no deben navegar por sitios de Internet que contengan material obsceno, odioso o censurable ni usar el correo electrónico para difundir materiales que sean ofensivos, obscenos, difamatorios, de naturaleza política o religiosa, o que estén destinados a molestar, acosar o intimidar a otra persona o personas. • Usar el correo electrónico o Internet para cualquier propósito ilegal, en contra de la política de la empresa o en contra del mejor interés de Intertek. • Transmitir o difundir información confidencial, materiales propietarios o secretos comerciales de Intertek a cualquier fuente externa sin un propósito comercial expreso o autorización. • Recibir o reenviar correos electrónicos no solicitados que violen la política de Intertek. • Intentar eludir cualquier mecanismo de seguridad para obtener acceso no autorizado a archivos informáticos u otra información en los sistemas o equipos de Intertek. • Publicar o transmitir cualquier mensaje de negocios o de Intertek de forma anónima o bajo un nombre falso, o permitir que cualquier otra persona lo haga. • Suplantar a otra persona a menos que sea como delegado autorizado. • Recopilar información sobre otros, incluidas direcciones de correo electrónico, sin su consentimiento. • Registrar direcciones de correo electrónico de Intertek para uso personal en sitios web de terceros no relacionados con el negocio, ya que esto es un riesgo de seguridad para Intertek y también puede llevar a correos electrónicos no solicitados (SPAM) posteriores. • Interceptar, grabar, leer, escuchar, alterar o recibir el correo electrónico de otro usuario sin autorización y para un propósito legítimo y proporcionado.	**CDRP7**

	• Usar proxies no autorizados para acceder a cualquier sitio de Internet. • Realizar una navegación personal excesiva, como en sitios de redes sociales, wikis, blogs, etc. • Realizar negocios personales durante el horario de trabajo o con propiedad de la empresa.	
AUT14	**Correo Electrónico de Remitente Desconocido** Los usuarios NO DEBEN abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos o sospechosos, que pueden contener virus, bombas de correo electrónico o códigos maliciosos. Notificar al Equipo Global de Ciberseguridad (CSHub@intertek.com) sobre cualquier correo electrónico sospechoso o inquietudes relacionadas. El botón "Reportar Phishing" en Outlook también puede usarse para informar sobre correos electrónicos de phishing sospechosos al Equipo Global de Ciberseguridad.	**CDRP7**
AUT15	**Actividad del Sistema y la Red** **Los usuarios no deben:** • Conectar dispositivos de cómputo personales a los equipos o redes de Intertek o cargar software en ellos sin la aprobación previa por escrito del Departamento de TI. • Cargar datos o programas de Intertek en computadoras personales o cualquier otro equipo que no pertenezca a Intertek, a menos que esté formalmente aprobado por el Departamento de TI. • Exportar software, información técnica, software de cifrado o tecnología, en violación de las leyes de control de exportación internacionales o regionales. • Introducir intencionalmente software y programas dañinos o maliciosos (por ejemplo, virus, gusanos, caballos de Troya, bombas de correo electrónico). • Copiar, almacenar o transmitir materiales con derechos de autor sin el permiso del titular de los derechos. • Usar una red o dispositivo de Intertek para ver, adquirir o transmitir material, o para cualquier propósito que viole cualquier ley aplicable. • Efectuar violaciones de seguridad o interrupciones de las comunicaciones. Las "violaciones de seguridad" incluyen, entre otros, el acceso no autorizado a datos; las "interrupciones" incluyen, entre otros, el sniffing de red, inundaciones de ping, suplantación de paquetes, denegación de servicio y falsificación de información de enrutamiento. • Realizar escaneos de puertos o seguridad no autorizados, monitoreo de red o intercepción de datos. • Eludir la autenticación de usuarios o la seguridad de cualquier host, red o cuenta.	**CDRP7**

	• Interferir o negar el servicio a cualquier usuario (por ejemplo, ataque de denegación de servicio) o usar cualquier programa/script/comando o mensaje con la intención de interferir o deshabilitar la sesión de terminal de un usuario. • Proporcionar propiedad de la empresa, incluidos datos confidenciales, a cualquier fuente externa.	
8.4 NOTIFICACIÓN DE USO INDEBIDO		
AUT16	Los usuarios deben notificar inmediatamente a un gerente senior de Intertek y/o al Departamento de TI si tienen motivos para cuestionar el uso de cualquier sistema, equipo o red de Intertek o si se enteran de cualquier mal uso de estos. Los usuarios acuerdan cuidar cualquier equipo de Intertek y no descuidarlo, desperdiciarlo, usarlo indebidamente o destruirlo, ya que constituye propiedad de Intertek. Un usuario que haya dañado su equipo asignado puede ser responsable ante Intertek por el costo de reemplazo. Las preguntas o inquietudes sobre esta política pueden dirigirse al Departamento de Recursos Humanos o al Departamento de TI.	**CDRP7**
8.5 VIOLACIÓN DE DATOS PERSONALES		
AUT17	En caso de una violación de datos personales relacionada con el uso de los Activos y Recursos Tecnológicos de Intertek, el usuario también debe informar, lo antes posible, la violación a su gerente directo y a Intertek IT [Reportar una Violación], cuando corresponda, de acuerdo con las políticas y procedimientos de Intertek.	**CDRP7**
8.6 DAÑO, PÉRDIDA Y ROBO		
AUT18	Es responsabilidad de los usuarios tomar las precauciones adecuadas para evitar daños, pérdidas o robo de un dispositivo de Intertek. Si un dispositivo se pierde, es robado, destruido o se sospecha que ha sido comprometido de alguna manera, el usuario debe notificar inmediatamente a Intertek IT y a su gerente de departamento dentro de las 24 horas. En caso de robo de un dispositivo de trabajo de Intertek, se debe presentar un informe policial.	**CDRP7**
8.7 MENSAJERÍA INSTANTÁNEA / HERRAMIENTAS DE COLABORACIÓN		
AUT19	Los empleados de Intertek no deben realizar negocios confidenciales a través de aplicaciones de mensajería instantánea que no estén aprobadas globalmente. Para cualquier decisión comercial tomada utilizando aplicaciones de mensajería instantánea de terceros (por ejemplo, WhatsApp y otras), el usuario es responsable de archivar las comunicaciones comerciales según la Política de Retención de Intertek. (Nota: solo se debe usar WhatsApp comercial, no personal). Las comunicaciones comerciales importantes, como acuerdos con clientes, contratos y aprobaciones deben guardarse imprimiéndolas en un archivo PDF o en una copia en papel si es necesario. Archivar estas comunicaciones es responsabilidad del usuario. • Los empleados deben usar Microsoft Teams entre empleados y terceros, en la medida de lo posible. Cuando el empleado tenga que usar una aplicación de conferencia no estándar de Intertek, como Zoom, deben seguirse las siguientes prácticas de seguridad:	

	○ Asegurarse de que todos los participantes en la lista de llamadas se identifiquen. ○ Usar una contraseña para proteger el acceso a la reunión. ○ No abrir enlaces ni archivos adjuntos no confiables. ○ Usar la cámara solo cuando sea necesario. ○ Restringir el uso compartido de archivos, el uso compartido de pantalla y la grabación. ○ Usar la versión más actualizada de la aplicación. ○ No discutir información sensible. • Durante las reuniones virtuales con partes externas y múltiples usuarios de Intertek, no se deben discutir otros temas de trabajo que no se relacionen con el tema en discusión mientras se espera que comience la reunión o durante otras pausas en la reunión.	

9. GLOSARIO

Acceso Administrativo - El acceso administrativo se refiere a cuentas con la capacidad de modificar el hardware y la configuración del sistema operativo de una computadora, que están por encima del nivel de las capacidades de un usuario regular en el sistema dado. Algunos sistemas pueden referirse a esto como acceso "root", "administrador" o "elevado".

Malware - Software o firmware destinado a realizar un proceso no autorizado que tendrá impactos adversos en la confidencialidad, integridad o disponibilidad de un sistema. Un virus, gusano, caballo de Troya, ransomware u otra entidad basada en código que infecta un host. El spyware y algunas formas de adware también son ejemplos de código malicioso.

Microsoft Active Directory - Es un servicio de directorio desarrollado por Microsoft para redes de dominio Windows. Está incluido en la mayoría de los sistemas operativos Windows Server como un conjunto de procesos y servicios.

10. ACEPTACIÓN DE LA POLÍTICA DE USO ACEPTABLE

Como condición de empleo, los empleados deben seguir la Política de Uso Aceptable de TI del Grupo Intertek o arriesgarse a acciones disciplinarias, incluidas el despido. Los contratistas deben seguir la Política de Uso Aceptable de TI del Grupo Intertek o arriesgarse a la terminación de su contrato. La empresa se reserva el derecho de informar cualquier violación ilegal a las autoridades correspondientes.

Certifico que he leído la Política de Uso Aceptable de TI del Grupo Intertek adjunta y, hasta donde sé, entiendo su intención, significado y mis responsabilidades bajo la misma. He tenido la oportunidad de hacer preguntas y buscar aclaraciones.

Firma: _____

Nombre Completo: _____

Fecha: _____

Oficina: _____

11. HISTORIAL Y APROBACIÓN DE DOCUMENTOS.

11.1. Revisions Control

VERSION	DATE	NAME	SUMMARY OF CHANGES
1.0	06/11/2009	Robert Jacobs	
1	06/11/2009	Andrew Hottes	
1.1	07/30/2009	Robert Jacobs	
1.1	07/30/2009	Andrew Hottes	
1.2	10/15/2009	Robert Jacobs	
1.2	10/16/2009	Andrew Hottes	
1.2	10/20/2009	Graham Lee	
1.2	10/20/2009	Rick Huntly	
1.2	10/26/2009	Carolyn Russell	
1.2	10/29/2009	Andrew Hottes	
1.3	10/30/2009	Robert Jacobs	
1.3	10/30/2009	Robert Jacobs	
1.3	11/16/2009	Andrew Hottes	
1.3	11/19/2009	Graham Lee	
1.4	12/01/2009	Robert Jacobs	
1.4		Andrew Hottes	Review for IOC Ratification.
2.1	08/08/2011	Joachim Zwick	
2.2		Ann-Michelle Bowlin	Review for IOC Ratification.
3.0	06/30/2013	D. Stanowick	Added "unless prohibited by law" to section 4.3.1.
3.1	08/2013	D. Stanowick	Formatting modifications and minor updates per recommendations from InfoTech.
3.2	09/2013	C. Stephens	Formatting modifications.
3.3	10/2014	A. Powell	Added Skype-related bullet point to section 4.3.6, per Group HR and CIO.
3.4	12/12/2019	Gerrie de Lange	Format changes and minor adjustments prior to full 2020 refresh of policies and procedures.
3.5	03/2021	C. Okonkwo	Minor updates.
3.5	03/2021	Gerrie de Lange	
3.6	11/2021	C. Okonkwo	Alignment with new policy template.
3.7	08/2022	Gerrie de Lange	Review and updates as part of 2022 annual cycle.
3.8	07/2023	C. Okonkwo	Updates
3.8	08/2023	Q. VanBenschoten	Revisions to content
3.8	09/2023	L. Atherton	Revisions to content

11.2. Scheduled Document Review

DATE OF NEXT SCHEDULED REVIEW	DESCRIPTION OF REVIEW TO BE PERFORMED
11/2024	Annual Review Cycle.

11.3. Approval

VERSION	NAME	POSITION	SIGNATURE	DATE
3.5	Gerrie de Lange	Global Head of Cyber Governance, Risk & Compliance (GRC)		03/2021
3.6	Gerrie de Lange	Global Head of Cyber Governance, Risk & Compliance (GRC)		12/2021
3.6	John Muller	Sr. Director IT Delivery and Operations	MS Teams Approval	-
3.6	Jed Kozicki	Head of IT Security Operations	MS Teams Approval	7 February 2022
3.6	Mark Thomas	Group General Counsel, and Head of Risk & Compliance	MS Teams Approval	7 February 2022
3.6	Q VanBenschoten	Vice President, Compliance and Risk - AMER	MS Teams Approval	-
3.7	Gerrie de Lange	Global Head of Cyber Governance, Risk & Compliance (GRC)		12/2022
3.7	Yvan Cordillet	Applications Development Director	MS Teams Approval	-
3.7	Mark Thomas	Group General Counsel, and Head of Risk & Compliance	MS Teams Approval	-
3.7	Q VanBenschoten	Vice President, Compliance and Risk - AMER	MS Teams Approval	12/2022

3.7	Amanda Bellgardt	Vice President, Human Resources USA & Canada	MS Teams Approval	-
3.7	Cristina Dutra	Compliance Manager		01/2023
3.7	Sally Murtagh	Director - Group Internal Communications		01/2023
3.7	Jedrzej Kozicki	Head of IT Security Operations	MS Teams Approval	12/2022
3.8	Yvan Cordillet	Applications Development Director		12/2023
3.8	Q VanBenschoten	Vice President, Compliance and Risk - AMER		12/2023
3.8	Amanda Bellgardt	Vice President, Human Resources USA & Canada		01/2024*
3.8	Laura Atherton	Group General Counsel		09/2023
3.8	Marie Giannini	VP Communications		01/2024*
3.8	Jedrzej Kozicki	Head of IT Security Operations		12/2023

11.4. Distribución

Esta política está disponible para todos los empleados de Intertek a través del Intranet de Intertek. Para acceder directamente a esta política en el Intranet, por favor navegue a:
https://intranet.intertek.com/Functions/IT/Policies/InformationSecurityPolicyFramework/