Las computadoras del sistema escolar, las redes y otros recursos tecnológicos apoyan las funciones educativas y administrativas del sistema escolar. Debido a que los empleados y los estudiantes dependen de estos sistemas para ayudar con la enseñanza y el aprendizaje y porque la información sensible y confidencial puede ser almacenada en estos sistemas, la integridad del sistema y la seguridad es de suma importancia.

A. SEGURIDAD DE LA RED Y LA INFORMACIÓN

Los sistemas de tecnología de la información del sistema escolar son activos valiosos que deben ser protegidos. Con este fin, el personal de tecnología escolar evaluará cada activo de tecnología de la información y asignará controles de protección que sean proporcionales al valor establecido de dichos activos. Deben establecerse medidas de seguridad adecuada para proteger todos los activos de tecnología de la información del uso, robo, modificación o destrucción accidental o no autorizado y para prevenir la divulgación no autorizada de información restringida. Las medidas de seguridad de la red deben incluir un proceso de recuperación de desastres del sistema de tecnología de la información. Las auditorías de las medidas de seguridad deben realizarse anualmente.

Todo el personal debe garantizar la protección y seguridad de los activos de tecnología de la información que están bajo su control.

B. CONOCIMIENTO DE SEGURIDAD

El director de tecnología o persona designada proporcionará a los empleados información para mejorar el conocimiento sobre amenazas a la seguridad tecnológica y para educarlos sobre las salvaguardias apropiadas, la seguridad de la red y la seguridad de la información.

C. PROTECCIÓN DE MALWARE

Los programas y prácticas de detección de malware deben implementarse en todo el sistema escolar. El superintendente o designado es responsable de asegurar que la red del sistema escolar incluya software actual para prevenir la introducción o propagación de malware informático.

D. FORMACIÓN PARA EL USO DE RECURSOS

Los usuarios deben ser capacitados como sea necesario para usar los recursos tecnológicos de manera efectiva y de una manera que mantenga la seguridad de la infraestructura de la red y asegure el cumplimiento con las leyes y regulaciones estatales y federales. Dicha capacitación debe incluir información relacionada con acceso remoto, protección antivirus, información del estudiante estatal y aplicaciones del sistema de mejoramiento educativo, seguridad de la red y de la información y otros temas que el superintendente o director de tecnología considere necesarios. La capacitación puede ser realizada como parte del programa de desarrollo profesional relacionado con la tecnología (ver política 3220, Tecnología en el Programa Educativo).

E. ACCESO A INFORMACIÓN DE SISTEMAS TECNOLÓGICOS

El acceso a los activos de tecnología de la información del sistema escolar se controlará y

Logró asegurar que sólo los dispositivos / personas autorizadas tengan acceso.

1. ID de usuario y contraseña

Todos los usuarios de sistemas de tecnología de la información deben estar debidamente identificados y autenticados antes de poder acceder a dichos sistemas. La combinación de una identificación de usuario única y una contraseña válida es el requisito mínimo para conceder acceso a sistemas de tecnología de la información. Dependiendo del entorno operativo, la información involucrada y los riesgos de exposición, se pueden requerir prácticas de seguridad adicional o más estricta según lo determine el superintendente o el director de tecnología. El director de tecnología o persona designada establecerá las capacidades y procedimientos de administración de contraseñas para garantizar la seguridad de las contraseñas.

2. Sistema de Información Estudiantil

El director de tecnología o persona designada debe asegurarse de que todas las computadoras del sistema escolar con acceso a la aplicación estatal de sistema de información para estudiantes conforme a la Política de Educación TCS-C-018 cumplan con las normas y requisitos pertinentes establecidos por la Junta Estatal de Educación, A la identificación del usuario, y las normas de seguridad de contraseña y estación de trabajo. Los empleados deben seguir todos estos estándares cuando usan cualquier computadora para acceder al sistema de información del estudiante, incluyendo cuando usan el computador personal del empleado.

3. Acceso Remoto

El superintendente y director de tecnología puede otorgar acceso remoto a usuarios autorizados de los sistemas informáticos del sistema escolar. El director de tecnología o persona designada debe asegurarse de que dicho acceso se proporciona a través de métodos de acceso seguros, autenticados y cuidadosamente administrados.

Referencias legales: G.S. 115C-523,-524; Junta Estatal de Educación Política TCS-C-018

Referencias: Profesional y Desarrollo del Personal (política de 1610/7800), Tecnología en el Programa Educativo (política 3220), Uso Responsable de Tecnología (política 3225/4312/7320), Internet Seguridad (política 3226/4205), Plan de Mejoramiento Escolar (política 3430), Uso de Equipos, Materiales y Suministros (política 6520)

Otras referencias: *Estado de Carolina del Norte Manual Estatal de Información de Seguridad* en (Oficina de Seguridad Empresarial y Gestión de Riesgos), disponible en http://it.nc.gov/document/statewide-information-security-manual

Aprobado: 20 de enero de 2009

Revisado: 30 de junio de 2009; 29 de agosto de 2012, 12 de diciembre de 2013, 12 de marzo de 2015, 09 de febrero de 2017