



EMAIL ARCHIVING

INTEGRIDAD Y CONFORMIDAD DE LOS DATOS DE CORREO ELECTRÓNICO PARA M365 Y OTROS SERVIDORES





Archivar los correos electrónicos de la empresa es una necesidad legal que debe cumplir varios requisitos. El archivado debe ser a prueba de auditoría y conforme a la ley, con períodos de conservación adecuados. Las tareas administrativas relacionadas con el archivado pueden llevar mucho tiempo, y los clientes necesitan una forma práctica de conceder acceso a terceros para realizar auditorías.

 Conforme a la legalidad

 Totalmente automático

 A prueba de fallos

ENTORNO DE CORREO ELECTRÓNICO

-  Archivado de correo electrónico en todo el dominio, conforme a la ley.
-  Acceso de doble control (4-eye) concedido para los requisitos de auditoría.
-  Acceso de auditoría limitado en el tiempo para auditores externos, conforme a los requisitos jurisdiccionales.
-  Archivado de correo electrónico sin esfuerzo, a prueba de revisiones y conforme a la legislación (GDPR, ISO).

AMPLIAS FUNCIONES PARA EL ALMACENAMIENTO SEGURO Y LEGAL DE CORREOS ELECTRÓNICOS:

Cifrado de la ruta de transmisión entre el archivo y el servidor de correo a través de TLS: Si el servidor de correo electrónico lo permite, los datos se codifican mediante TLS durante su transmisión para protegerlos contra cambios de contenido y archivos adjuntos.

Archivo automático, sin cambios ni modificaciones: Con un archivo a prueba de auditorías, todos los correos electrónicos entrantes y salientes se almacenan automáticamente en su forma original directamente a su llegada y envío en los centros informáticos de Hornetsecurity.

Omisión de los usuarios individuales del archivo: Para cumplir con las normativas de protección de datos, puede omitirse, por ejemplo, el comité de empresa del archivo automático de correo electrónico.



EMAIL ARCHIVING

AMPLIAS FUNCIONES PARA EL ALMACENAMIENTO SEGURO Y LEGAL DE CORREOS ELECTRÓNICOS:

Regular los plazos de conservación: Configurar el plazo de archivo de 3 meses a 10 años para cumplir las normas de protección de datos de las diferentes áreas. Por ejemplo, el plazo de retención de los documentos sobre candidatos a un empleo puede limitarse a 6 meses.

Amplia búsqueda de texto completo en el archivo siguiendo varios criterios: Pueden utilizarse criterios de búsqueda individuales, como la fecha, el remitente, el destinatario y el asunto, para reducir los parámetros de búsqueda y determinar con precisión los mensajes que se buscan y encontrarlos más rápidamente.

Registro de auditoría/rastreo de auditoría: Registro de todos los accesos al archivo de correos electrónicos. Este contiene, entre otras cosas, el nombre de usuario y la dirección IP del usuario y no puede editarse ni eliminarse. El administrador puede ver el registro de auditoría en cualquier momento.

Acceso a la auditoría con el principio de revisión doble: El acceso al archivo a través del acceso de la auditoría otorga al auditor un acceso temporal. Cuando finaliza la comprobación, el administrador tiene acceso al registro de revisiones donde puede ver qué datos se han visto.

Recuperación y restablecimiento de correos electrónicos archivados: Si los correos electrónicos de un usuario se borran accidentalmente en el servidor de correo, pueden recuperarse desde el archivo.

Marcado de correos electrónicos privados por parte de los usuarios: Protección de los correos electrónicos personales contra el acceso de los auditores; sólo pueden ver el asunto.

Archivo de correos electrónicos internos (opcional): Los correos electrónicos internos archivados se almacenan a prueba de auditorías desde el momento en que se archivan y se pueden buscar y recuperar del mismo modo que los correos electrónicos entrantes y salientes.

Sin acceso al contenido para los administradores: Los administradores no tienen acceso a los correos electrónicos archivados de los usuarios. Sólo se pueden ver los metadatos.

Concesión de derechos: Un usuario puede permitir que otro usuario acceda a su archivo de correos electrónicos.

Archivo posterior de correos electrónicos antiguos mediante la función de importación: Los correos electrónicos y sus archivos adjuntos pueden importarse de otras bases de datos al archivo de correo electrónico de Hornetsecurity, ya sea en formato .pst u Outlook.

Exportación de los datos archivados en cualquier momento: Todo el archivo de correo electrónico puede exportarse fácilmente y en cualquier momento.

Clasificación clara de los archivos en caso de cambios de las direcciones de correo: Si un usuario recibe una nueva dirección de correo electrónico, los mensajes archivados pueden asignarse a esta nueva dirección para que el usuario pueda seguir accediendo a los datos.

Uso de Unicode: Los correos electrónicos se guardan en su formato original, la codificación no es importante. Esto se aplica a los diferentes idiomas y caracteres, así como a los mensajes cifrados.

Espacio de almacenamiento ilimitado por usuario: Cada usuario tiene acceso a un tamaño de archivado ilimitado, válido para todo el periodo de archivado.