POLÍTICA DE CONTRASEÑAS DE IT

RESUMEN

Las contraseñas son un aspecto importante de la seguridad informática. Una contraseña mal elegida puede resultar en el acceso no autorizado y / o la explotación de nuestros recursos. Todo el personal, incluidos los contratistas y proveedores con acceso a los sistemas Mister Car Wash, son responsables de tomar las medidas apropiadas como se describe a continuación para seleccionar y proteger sus contraseñas.
Esta política se basa en la plantilla estándar emitida por el Instituto SANS, una organización cooperativa de investigación y educación en seguridad (https://www.sans.org) y los Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) (https://www.pcisecuritystandards.org).

PROPÓSITO

El propósito de esta política es establecer un estándar para la creación y protección de contraseñas seguras.

OBJETIVO

El objetivo de esta política incluye a todo el personal que tiene o es responsable de una cuenta (o cualquier forma de acceso que admita o requiera una contraseña) en cualquier sistema que resida en cualquier instalación de Mister Car Wash, tenga acceso a la red de Mister Car Wash o almacene cualquier información no pública de Mister Car Wash.

DECLARACIÓN DE POLÍTICA

Creación de contraseñas

Las contraseñas deben cumplir con estos estándares:
• Tener una longitud mínima de 9 caracteres (las contraseñas de 14 caracteres o más son mejores).
• No contener información personal, incluyendo fechas de nacimiento, direcciones, números de teléfono o nombres de familiares, mascotas, amigos y personajes ficticios.
• No contienen patrones o secuencias fáciles de adivinar (por ejemplo, "aaabbb", "qwerty", 123321").
• No ser alguna versión de "Welcome123", "Password123", "Changeme123", etc.

Las frases de contraseña, que son contraseñas compuestas de varias palabras, son muy recomendables. Las frases de contraseña como "it'stimeforvacation" y "block_curious_sunny_leaves" cumplen con los estándares de contraseña enumerados anteriormente y son fáciles de recordar y escribir.

Directrices adicionales

• Los empleados deben usar una contraseña única y separada para cada cuenta relacionada con el trabajo que usen.
• Los empleados no pueden aplicar contraseñas relacionadas con el trabajo a sus cuentas personales.
• Se recomienda encarecidamente que se use alguna forma de autenticación multifactor para las cuentas con privilegios.
• No utilice valores predeterminados proporcionados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

Cambio de Contraseña

pPra cumplir con las regulaciones PCI en el Entorno de Datos del Titular de la Tarjeta (CDE):

• Las contraseñas deben cambiarse cada 90 días.
• Las contraseñas no pueden ser las mismas que cualquiera de las últimas 4 contraseñas utilizadas. • Las contraseñas también deben cambiarse cuando hay razones para creer que una contraseña ha sido comprometida.
• El descifrado o adivinar contraseñas puede ser realizado de forma periódica por Mister IT o sus delegados. Si una contraseña se adivina o se agrieta durante uno de estos análisis, el usuario deberá cambiarla.

Protección con Contraseña
• Las contraseñas no deben compartirse con nadie, incluidos los supervisores y compañeros de trabajo. Todas las contraseñas deben ser tratadas como información confidencial y confidencial de Mister.
• Las contraseñas no deben insertarse en mensajes de correo electrónico u otras formas de comunicación electrónica junto con cualquier información de identificación del usuario o del sistema.
• Las contraseñas sólo pueden almacenarse en "gestores de contraseñas" autorizados por la organización.
• No utilice la función "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web).
• Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe informar del incidente y cambiar todas las contraseñas.

Limitación de Tiempo

• Una cuenta se bloqueará después de 5 intentos fallidos.
• Después de que una cuenta se bloquee debido a intentos fallidos, la cuenta permanecerá bloqueada durante 30 minutos.

Desarrollo de Aplicaciones
Los desarrolladores de aplicaciones deben asegurarse de que sus programas contienen las siguientes precauciones de seguridad:

• Las aplicaciones deben admitir la autenticación de usuarios individuales, no de grupos.
• Las aplicaciones no deben almacenar contraseñas en texto no cifrado ni en ninguna forma fácilmente reversible.
• Las aplicaciones no deben transmitir contraseñas en texto no cifrado a través de la red.
• Las aplicaciones deben prever algún tipo de administración de roles de tal manera que un usuario pueda hacerse cargo de las funciones de otro sin tener que conocer la contraseña del otro.

Autenticación Multifactor

• La autenticación multifactor es muy recomendable y debe usarse siempre que sea posible, no solo para cuentas relacionadas con el trabajo, sino también para cuentas personales.

Cumplimiento

Mister IT verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la directiva.

Cualquier excepción a esta política debe ser aprobada por el Departamento de IT de antemano.

Cualquier empleado que haya violado esta política puede estar sujeto a acciones disciplinarias hasta e incluyendo la terminación del empleo.

Excepciones
- Carta
- Uso de Jira por parte de Inspyrus para la gestión de cambios
- Uso de ServiceNow para la gestión de cambios

DEFINICIONES

Autenticación Multifactor (MFA)
Un método de autenticación que requiere más de una forma de validación para verificar la identidad del usuario para un inicio de sesión u otra transacción.

Manejo de Contraseñas
Una aplicación de software o un dispositivo de hardware que se utiliza para almacenar y administrar las contraseñas de una persona. Normalmente, las contraseñas almacenadas se cifran.

POLÍTICAS, PROCEDIMIENTOS Y FORMULARIOS RELACIONADOS
- Política de Uso Aceptable (IT.4000-MCW-POL)
- Reconocimiento de Uso Aceptable (IT.4000.1-MCW-FRM)

REVISIÓN
Esta política se revisará **anualmente** y se actualizará según sea necesario

Nombre y Puesto	Fecha
Lauren Babson, Vice President of Information Technology	2021-01

APROBACIÓN

Only a representative from the Policy Review Committee can approve a policy following the procedure set forth in GRC.100.1-MCW-PRC.

Nombre, Puesto y Firma	Fecha
Lauren Babson Lauren Babson, Vice Presidente de Informática y Tecnología	2021-01

HISTORIAL

Versión	Expedición	Actualizado por	Revisiónes
Rev. 4	2021-01	Lauren Babson	Se agregó la sección limitación de tiempo & Excepciones para aplicaciones que no pueden cumplir que se encuentran dentro del ámbito de auditoría SOX
Rev. 3	2019-09	Lucas Schippers	Formato de documento actualizado para que coincida con Mister estándares de formato de políticas/procedimientos. Número de política asignado. Se ha movido la información del "Apéndice A: Directrices para la construcción de contraseñas" al cuerpo de la política.
Rev. 2	2018-07	Lauren Babson	Se actualizó para reflejar los nuevos estándares NIST SP800-63.3 y PCI DSS.
Rev. 1	2017-02	Jeff Parry	Docuemnto creado.