Diretrizes de Segurança da Informação para Fornecedores

KSU/ CSD 2.5

Public

ÍNDICE

1. Objetivo 3
1.1. Estrutura de documentos e público alvo 3
1.2. Área de Aplicação 3
2. Visão Geral do Processo 4
2.1. Requerimentos Gerais para todos os Terceiros 4
2.2. Requerimentos Adicionais 4
2.3. Requisitos adicionais para terceiros que trabalham na infraestrutura do Grupo Volkswagen ... 5
2.4. Definição 5
2.5. Requisitos 6
2.6. Tratamento com informações Classificadas 8
2.7. Tratamento de contas de usuário 13
2.8. Uso de Serviços de Rede 13
2.9. Requisitos adicionais para trabalho remoto 14
2.10. Requisitos adicionais para terceiros que tenham ou fornecem acesso às informações do Grupo Volkswagen fora da infraestrutura da Volkswagen 15
2.11. Definições 15
2.12. Requisitos 15
2.13. Responsabilidades 15

1. Objetivo

As diretrizes de segurança da informação definem as regras de segurança da informação que terceiros devem observar ao usar informações e dispositivos de TI (ex.: computadores pessoais, estações de trabalho, smartphones ou tablets).

Terceiros são definidos como qualquer parte que forneça serviços para o Grupo Volkswagen com base em uma relação contratual. Empresas subsidiárias, marcas do Grupo Volkswagen e companhias que são majoritariamente pertencentes ao Grupo Volkswagen são excluídas de tal definição.

1.1. Estrutura de documentos e público alvo

Essas diretrizes são voltadas para a administração de terceiros, funcionários e subcontratados relevantes. A administração de terceiros deve garantir que seus funcionários e agentes indiretos que processam informações do Grupo Volkswagen estejam vinculados a esta diretriz.

Esta diretriz não se aplica a clientes de uma empresa do Grupo Volkswagen.

O documento contém três capítulos. A tabela abaixo lista a estrutura do documento e o público-alvo de cada capítulo.

Capítulo	Público alvo
1	Todos os terceiros
2	Terceiros que usam infraestrutura Volkswagen
3	Terceiros que acessam ou forneçam dados e informações da Volkswagen fora da infraestrutura Volkswagen

Um terceiro pode pertencer a mais de uma categoria

1.2. Área de Aplicação

Estas instruções aplicam-se a todos os terceiros que processam informações classificadas como internas, confidenciais ou secretas para o Grupo Volkswagen de acordo com acordos contratuais.

2. Visão Geral do Processo

2.1. Requerimentos Gerais para todos os Terceiros

O objetivo da classificação é classificar as informações em etapas, dependendo de sua necessidade de proteção. Dependendo da classificação, diferentes medidas de proteção são necessárias.

Todas as informações do Grupo Volkswagen devem ser classificadas de acordo com a confidencialidade. As classificações de confidencialidade podem mudar em determinados marcos.

Se documentos ou informações forem preparados por terceiros para o Grupo Volkswagen, a classificação de acordo com a confidencialidade deve ser solicitada à pessoa responsável do Grupo Volkswagen e registrado o de acordo.

2.2. Requerimentos Adicionais

- Eventos de segurança da informação (por exemplo, mau funcionamento que ocorrem, violações dos regulamentos de segurança da informação, ataques cibernéticos) relativos a informações ou sistemas de TI do cliente devem ser relatados imediatamente à autoridade competente com as informações necessárias para avaliar a criticidade (ver Anexo B.1.1). Mais informações sobre o evento devem ser disponibilizadas ao cliente mediante solicitação.

- Se houver suspeita ou detecção de um ataque usando malware, os dispositivos de TI e a mídia de armazenamento afetados não poderão mais ser utilizados para processar informações do Grupo Volkswagen.

- As suspeitas de vulnerabilidades e fraquezas dos sistemas informáticos do cliente devem ser comunicadas imediatamente à autoridade competente (ver anexo B.1.1)

- Se houver suspeita de perda de informações internas, confidenciais ou secretas do cliente, isso deve ser comunicado imediatamente à pessoa de contato da empresa do Grupo Volkswagen comissionadora.

- A transferência de dados ou informações para terceiros só é permitida com

INTERNAL

a aprovação por escrito do proprietário das informações (consulte o Apêndice B.1.3).

- Documentos e mídias de armazenamento com informações confidenciais do Grupo Volkswagen devem ser protegidos contra perda, destruição e alterações indevidas, bem como contra acesso não autorizado. Assim que os dados no suporte de armazenamento não forem mais necessários, os dados devem ser excluídos com segurança (substituindo sete vezes ou por um desmagnetizador). A mídia de armazenamento que não é mais necessária deve ser destruída fisicamente.

- Em todas as conversas e transmissões de dados (incluindo chamadas telefônicas, videoconferências e webconferências) que digam respeito ou contenham informações confidenciais ou secretas do Grupo Volkswagen, deve-se garantir que não possam ser ouvidas ou lidas sem autorização.

- Informações confidenciais ou secretas não podem ser usadas como parte de nomes de arquivos ou em linhas de assunto de e-mail.

- O processamento de informações sem erros e a proteção contra alterações não autorizadas devem ser garantidos.

2.3. Requisitos adicionais para terceiros que trabalham na infraestrutura do Grupo Volkswagen

2.4. Definição

A terceiro trabalha na infraestrutura do Grupo Volkswagen se:

- Equipamentos de TI (dispositivos finais físicos ou virtuais) são fornecidos por uma empresa do Grupo Volkswagen.

Ou

- A conexão via soluções de acesso remoto com acesso à rede interna do grupo.

Ou

- O terceiro está conectado diretamente à rede interna do grupo .

Ou

- Quando são utilizadas aplicações protegidas por acesso de uma empresa do Grupo Volkswagen fornecidas através da Internet. Isso não se aplica a aplicativos usados pelo usuário em sua função de cliente final.

Isso se aplica independentemente de o terceiro estar localizado nas instalações de uma empresa do Grupo.

2.5. Requisitos

- Devem ser cumpridos os regulamentos da respectiva empresa do Grupo relativos à transferência de equipamentos de TI não pertencentes à respectiva empresa do Grupo para as instalações da empresa ou em áreas de segurança.

- Os equipamentos de TI fornecidos pela respectiva empresa do Grupo devem ser tratados adequadamente e protegidos contra perda ou alteração não autorizada.

- Os regulamentos do fabricante para a proteção de equipamentos de TI devem ser cumpridos.

- O equipamento de TI fornecido pela respectiva empresa do Grupo só pode ser retirado das instalações da fábrica da empresa do Grupo após a aprovação.

- O fornecimento ou instalação de hardware e software só pode ser realizado ou iniciado pelo departamento da empresa do Grupo responsável por eles.

- No que diz respeito ao uso do hardware e software fornecidos pela respectiva empresa do Grupo, aplicam-se os regulamentos da respectiva empresa do Grupo.

- Somente o uso de hardware, software e mídia de armazenamento fornecidos pela respectiva empresa do Grupo é permitido. As exceções podem ser discutidas em casos individuais com a pessoa de contato responsável no departamento de comissionamento da empresa do Grupo. As exceções para fins de acesso à rede do Grupo,

acesso remoto ou trabalho móvel são descritas no Capítulo 2.4.

- Abrir o equipamento de TI fornecido pela respectiva empresa do Grupo e fazer alterações no hardware (por exemplo, instalar/remover componentes) e alterar as configurações de segurança (por exemplo, no navegador da web) só é permitido às autoridades responsáveis do Grupo Volkswagen. A remoção de restrições de uso (por exemplo, "jailbreaking" ou "root do sistema operacional") não é permitida.

- O uso ou modificação subsequente de programas da respectiva empresa do Grupo só é permitido se isso tiver sido aprovado pela pessoa de contato responsável no departamento de comissionamento da empresa do Grupo.

- Nenhum dado de outros clientes que não pertençam ao Grupo pode ser processado nos equipamentos de TI fornecidos pela respectiva empresa do Grupo.

- Cada terceiro é responsável por garantir que as informações, programas e equipamentos de TI sejam usados e usados adequadamente apenas no escopo da respectiva tarefa.

  • Não é permitido o envio de informações não oficiais.

  • Não é permitido o uso de software e dados privados sobre os equipamentos de TI fornecidos pela respectiva empresa do Grupo.

- A utilização de equipamentos ou dados informáticos da respetiva empresa do grupo por colaboradores de terceiros requer o consentimento expresso da respetiva empresa do grupo. A respectiva empresa do Grupo está autorizada a proibir o acesso ou uso a qualquer momento (por exemplo, em caso de uso indevido).

- O hardware que não é mais necessário (por exemplo, laptop, cartões inteligentes, tokens SecurID, pen drives, discos USB) e o software devem ser devolvidos à respectiva empresa do Grupo imediatamente, até o final do contrato.

- As reparações de periféricos e computadores fornecidos pela empresa do Grupo só podem ser exexutada pela empresa do Grupo.

- A perda de hardware fornecido pela empresa do Grupo deve ser

comunicada imediatamente pelo usuário correspondente à pessoa de contato responsável no departamento de comissionamento da empresa do Grupo.

- O armazenamento de dados não classificados publicamente de propriedade da empresa só é permitido em mídias de armazenamento aprovadas (por exemplo, arquivos compartilhados ou serviços de armazenamento em nuvem homologados).

- A coleta, tratamento ou utilização de dados pessoais (por exemplo, nome, número de telefone, endereço de e-mail, data de nascimento) só é permitida se

  o houver consentimento do titular dos dados (pessoa física).

  ou

  o Existe uma base jurídica para tal.

- Os dados pessoais armazenados em uma empresa do grupo só podem ser processados e usados no âmbito das atividades acordadas contratualmente. Não é permitida a transferência desses dados para pessoas não autorizadas.

- Os dispositivos de TI e os suportes de dados nos quais são armazenados dados pessoais, confidenciais ou secretos só podem sair das propriedades do Grupo Volkswagen de forma criptografada.

2.6. Tratamento com informações Classificadas

As informações só podem ser disponibilizadas a um grupo autorizado de pessoas para efeitos das atividades acordadas e em conformidade com a regulamentação aplicável. O princípio do need-to-know deve ser seguido.

Para proteger informações internas, confidenciais ou sigilosas, o computador deve ser configurado de forma a impedir acessos não autorizados e reduzir ao máximo o risco de exposição a pessoas não autorizadas.

As informações devem ser protegidas contra o acesso de pessoas não autorizadas durante todo o seu ciclo de vida, de acordo com seu nível atual de confidencialidade.

Aplicam-se os seguintes regulamentos:

Classificação	**Requisitos**
Público	• Marcação/Classificação: nenhuma/opcional (por exemplo, nota na impressão) • Reprodução e distribuição: sem restrições • Armazenamento: sem restrições • Descarte: sem restrições
Interno	• Marcação/Classificação: Indicação do nível de confidencialidade "Interno" ou "Interno" na primeira página do documento • Reprodução e distribuição: apenas a funcionários autorizados do Grupo e terceiros autorizados no âmbito da atividade ou no âmbito de aplicação • Armazenamento: Proteção contra acesso não autorizado • Descarte: De acordo com a ISO/IEC 21964, classe de proteção 1
Confidencial	• Marcação/Classificação: Indicação do nível de confidencialidade "Confidencial"

	ou "Confidencial" em cada página do documento • Reprodução e distribuição: apenas para um grupo limitado de funcionários autorizados do Grupo e terceiros autorizados no âmbito da atividade e âmbito de aplicação. A pessoa que distribui as informações é responsável pelos canais de distribuição apropriados para proteger as informações e os dados contra acesso não autorizado e/ou espionagem (por exemplo, Confidencial usando criptografia). • Armazenamento: Acesso apenas para um grupo limitado de funcionários autorizados do Grupo e terceiros autorizados dentro do escopo da atividade e do escopo de aplicação (por exemplo, por grupos fechados de usuários). Devem ser utilizados suportes de armazenamento adequados. • Descarte: De acordo com a ISO/IEC 21964, classe de proteção 2 • Transporte/Envio: Documentos confidenciais e mídia de armazenamento devem ser enviados em envelopes lacrados e neutros. Se necessário, a adição "pessoal" pode ser adicionada. Isso significa que o envelope só pode ser aberto pela pessoa endereçada.

	• Impressão: Impressão somente sob a supervisão do impressor
Secreto	• Marcação/Classificação: Indicação do nível de confidencialidade "Segredo" ou "Segredo" em cada página do documento • Além disso, todas as páginas devem ser marcadas com "página x de y". • Reprodução e distribuição: apenas a um grupo extremamente limitado (por exemplo, lista por nome) de funcionários autorizados do Grupo e terceiros autorizados no âmbito da atividade ou âmbito de aplicação e com a aprovação prévia do proprietário da informação. Todos os dados devem ser criptografados. Dependendo da aplicação, outras medidas de proteção técnicas ou organizacionais devem ser usadas (por exemplo, proibição de compartilhamento, impressão, marcas da água. Devem ser utilizados meios de comunicação que impeçam a espionagem, como videoconferências com criptografia de ponta a ponta. • Armazenamento: Acesso apenas para um grupo extremamente limitado (por exemplo, lista por nome) de funcionários autorizados do Grupo e terceiros autorizados no âmbito da

	atividade e no âmbito da aplicação (por exemplo, por grupos fechados de usuários). Todos os dados devem ser criptografados. • Descarte: De acordo com a ISO/IEC 21964, classe de proteção 3 • Transporte: Documentos secretos e mídia de armazenamento devem ser enviados em envelopes externos neutros e lacrados (sem acréscimos como "pessoal, secreto, etc."). Um segundo envelope interno deve ser colocado neles, que é marcado com a classificação "segredo". Documentos secretos ou mídia de armazenamento eletrônico só podem ser retirados das instalações da empresa por funcionários autorizados a fazê-lo por escrito por seu respectivo gerente. • Impressão: Impressão somente sob a supervisão do impressor

Os requisitos para o tratamento da informação (rotulagem, duplicação, distribuição, armazenamento e eliminação) aplicam-se igualmente aos sistemas informáticos (por exemplo, bases de dados e suportes de cópia de segurança). Em particular, nenhum serviço público de tradução pela Internet pode ser usado para traduções de documentos contendo informações do Grupo Volkswagen.

2.7. Tratamento de contas de usuário

Os seguintes requisitos ao lidar com contas de usuário e senhas devem ser seguidos por todos os usuários:

- O uso da conta de usuário de outra pessoa não é permitido.
- As contas de usuário ou autorizações de acesso que não são mais necessárias devem ser comunicadas imediatamente à pessoa de contato responsável no departamento de comissionamento da empresa do Grupo para que possam ser excluídas ou bloqueadas.
- A transferência de meios de autenticação (por exemplo, cartões inteligentes, aplicativos autenticadores e tokens) não é permitida.
- Os dispositivos de autenticação que não são mais necessários devem ser devolvidos imediatamente à pessoa de contato responsável no departamento de comissionamento da empresa do Grupo.
- Senhas e PINs de uma conta de usuário destinada ao uso pessoal não podem ser compartilhados ou compartilhados.
- Assim que houver suspeita de comprometimento ou divulgação de uma senha ou PIN, esta ou mais devem ser alteradas imediatamente.
- Senhas ou PINs são classificados pelo menos confidencialmente. Para definir uma senha ou PIN, os seguintes requisitos devem ser atendidos:
    - Uma senha separada deve ser usada em cada sistema de TI que usa sua própria senha.
    - Em particular, não é permitido usar uma senha usada para fins comerciais para fins privados.
    - Senhas triviais (por exemplo, "Test12345678") ou senhas com referência pessoal (por exemplo, nome, data de nascimento) não são permitidas.

2.8. Uso de Serviços de Rede

Dispositivos com capacidade de rede fornecidos por empresas do Grupo Volkswagen só podem ser conectados a redes externas (como pontos de acesso, WLANs privadas ou redes móveis) mediante aprovação explícita da empresa responsável para o respectivo dispositivo.

A conexão de dispositivos com capacidade de rede à rede do Grupo só é permitida se este procedimento tiver sido explicitamente aprovado para o respectivo dispositivo pela empresa do Grupo.

2.9. Requisitos adicionais para trabalho remoto

Os funcionários de terceiros são responsáveis por garantir o cumprimento integral dos regulamentos aplicáveis à segurança da informação e proteção de dados, especialmente durante atividades de trabalho móvel. Documentos, dados e informações corporativas não devem ser visíveis ou acessíveis a pessoas não autorizadas, seja em locais públicos ou em ambientes privados, e devem estar protegidos contra interceptações.

Além disso, deve-se assegurar a proteção contra gravações por dispositivos de reconhecimento de voz. Como regra geral, informações classificadas como secretas não devem ser processadas durante o trabalho móvel

A conexão de hardwares (por exemplo, mouse, teclado, pendrive) ao hardware fornecido pela empresa do Grupo Volkswagen só é permitida se tiver sido fornecida pela empresa do Grupo Volkswagen.

Os dispositivos de saída de imagem (por exemplo, monitores, projetores) que não tenham sido fornecidos pela empresa do Grupo Volkswagen podem ser utilizados se a ligação estiver ligada e não for utilizada qualquer transmissão de rádio.

Fones de ouvido e sistemas viva-voz não fornecidos por empresas do Grupo Volkswagen só podem ser conectados aos dispositivos por meio da entrada de áudio (fone/microfone), sendo proibida a conexão via porta USB.

Os equipamentos de TI fornecidos pela respectiva empresa do Grupo devem estar fisicamente protegidos contra roubo e uso indevido, conforme as seguintes diretrizes:

- Caso um dispositivo seja deixado sem supervisão dentro de um veículo,

ele deve ser armazenado de forma que não fique visível do lado externo.

- Durante viagens aéreas ou ferroviárias, os equipamentos de TI devem ser transportados como bagagem de mão.

- Se o dispositivo permanecer sem supervisão por um período prolongado, ele deve ser desligado completamente.

2.10. Requisitos adicionais para terceiros que tenham ou fornecem acesso às informações do Grupo Volkswagen fora da infraestrutura da Volkswagen

2.11. Definições

Um terceiro tem acesso às informações do Grupo Volkswagen fora da infraestrutura do Grupo Volkswagen quando este Grupo Volkswagen processa informações em sua própria infraestrutura de TI.

2.12. Requisitos

Aplicam-se os regulamentos de segurança da informação do terceiro, salvo acordo contratual em contrário

2.13. Responsabilidades

Um terceiro Violações a esta diretriz serão analisadas individualmente, com base nas disposições legais e contratuais vigentes, e poderão ser punidas conforme aplicável.

Exceções que comprometam o nível de segurança só serão permitidas mediante consulta prévia com o responsável designado pela empresa do Grupo Volkswagen, devendo ser sempre autorizadas formalmente e limitadas a um período específico.