KRYPTOGRAFISCHE

KONTROLL POLITIK

[Betreff].

1 Versionskontrolle von Dokumenten

	Zuletzt geändert	Zuletzt geändert von	Änderungen des Dokuments
0.1	[DATUM]		Zum ersten Mal erstelltes Dokument

2 Index

3 Politik der kryptografischen Kontrolle

3.1 Zweck

Zweck dieser Richtlinie ist es, die korrekte und wirksame Verwendung von Verschlüsselung zum Schutz der Vertraulichkeit und Integrität vertraulicher Informationen sicherzustellen.

3.2 Empfänger

Vertrauliche und personenbezogene Daten, die auf oder in Systemen und Anwendungen verarbeitet, gespeichert oder übermittelt werden, die dem Unternehmen gehören, von ihm betrieben und kontrolliert werden und in den Geltungsbereich der Erklärung zum Geltungsbereich fallen

Alle Mitarbeiter und Drittnutzer.

3.3 Grundsatz

Der Schutz von Informationen erfolgt durch klassifizierungsbasierte Kontrollen, wie sie in der Klassifizierungs- und Informationsmanagementpolitik dargelegt sind und auf einer Risikobewertung basieren.

Es werden nur vom Unternehmen zugelassene Verschlüsselungsverfahren und -technologien verwendet.

Die Ausfuhr von Verschlüsselungstechnologien oder verschlüsselten Daten kann durch Rechtsvorschriften eingeschränkt sein. Die Mitarbeiter werden die Rechtsabteilung um

Unterstützung bitten, wenn die Ausfuhr von Verschlüsselungstechnologien oder verschlüsselten Daten erforderlich ist.

3.4 Anforderungen an den Verschlüsselungsalgorithmus

Symmetrische Verschlüsselung: AES-256 Bit

Asymmetrische Verschlüsselung: RSA (2048 Bit empfohlen, mindestens 1200 Bit erforderlich).

Hash-Funktionen: SHA2 (vier Dimensionen, 256 Bits empfohlen).

Digitale Signaturen: RSA (2048 Bit empfohlen, mindestens 1200 Bit erforderlich).

3.5 Verschlüsselung von mobilen Geräten, Laptops und Wechselmedien

Bei mobilen Geräten, Laptops und Wechselmedien wird die Festplattenverschlüsselung auf der Ebene der Hardware und/oder des herstellereigenen Betriebssystems implementiert.

Die Geräteverschlüsselung darf niemals deaktiviert werden.

Der Zugang zu verschlüsseltem Speicher auf mobilen Geräten muss durch ein Passwort, eine Passphrase, eine PIN oder einen anderen Authentifizierungsmechanismus geschützt werden.

Werden für den Zugriff auf den verschlüsselten Speicher allgemeine Passwörter verwendet, ist für den Zugriff auf das Gerät selbst eine eindeutige zweite Anmeldung erforderlich.

Zur Speicherung vertraulicher Daten dürfen nur verschlüsselte Geräte mit firmeneigenen und bereitgestellten Wechselmedien verwendet werden.

3.6 E-Mail-Verschlüsselung

E-Mails werden standardmäßig mit der x, y, z-Implementierung verschlüsselt bzw. nicht verschlüsselt.

E-Mails sollten nicht zur Übermittlung vertraulicher oder personenbezogener Daten in einem Format verwendet werden, das nicht gemäß der Informationsübertragungspolitik verschlüsselt ist.

Falls erforderlich, muss eine verschlüsselte Datei mit einer Schlüssellänge, die den Anforderungen des Verschlüsselungsalgorithmus entspricht, beigefügt werden.

3.7 Verschlüsselung von Web/Cloud-Diensten

Web- und Cloud-Dienste, die den Austausch vertraulicher, persönlicher oder sensibler Daten erfordern, müssen mindestens TLS 1.2 implementieren, um Daten bei der Übertragung über das Internet zu schützen.

Alle Server müssen über ein gültiges, von einer anerkannten Zertifizierungsstelle ausgestelltes Zertifikat verfügen. Es liegt in der Verantwortung des Systemeigentümers,

das Zertifikat zu erneuern und sicherzustellen, dass die Systeme auf dem neuesten Stand sind.

3.8 Drahtlose Verschlüsselung

WEP sollte nicht als Sicherheitskontrolle für drahtlose Netzwerke verwendet werden.

Für WLANs ist der WPA- oder WPA2-Enterprise-Modus mit 802.1X-Authentifizierung und AES-Verschlüsselung implementiert.

Es werden zentralisierte Verwaltungssysteme eingesetzt, die verteilte drahtlose Netze steuern und konfigurieren können.

Falls erforderlich, empfehlen wir die Verwendung des WPA2 Personal-Modus mit einer zufälligen Passphrase von mindestens 13 Zeichen und AES-Verschlüsselung.

3.9 Verschlüsselung von Karteninhaberdaten

Es speichert die geheimen und privaten Schlüssel, die immer zur Ver-/Entschlüsselung von Karteninhaberdaten verwendet werden, in einer (oder mehreren) der folgenden Formen:

- Verschlüsselt mit einem Schlüssel, der mindestens so sicher ist wie der Datenverschlüsselungsschlüssel und getrennt vom Datenverschlüsselungsschlüssel gespeichert wird
- innerhalb eines sicheren kryptografischen Geräts (z. B. ein Hardware-(Host-)Sicherheitsmodul (HSM) oder ein vom PTS zugelassenes Point-of-Interaction-Gerät)

- Mindestens zwei Schlüsselkomponenten oder Schlüsselanteile in voller Länge nach einer in der Branche anerkannten Methode

Hinweis: Die öffentlichen Schlüssel müssen nicht in einem dieser Module gespeichert werden.

3.10 Backup-Verschlüsselung

Die Backups werden mit der herstellereigenen Backup-Technologie verschlüsselt.

3.11 Verschlüsselung der Datenbank

Datenbanken, die vertrauliche Informationen oder personenbezogene Daten enthalten, werden im Ruhezustand auf der Ebene der Datenbankanwendung oder der Festplatte verschlüsselt.

3.12 Verschlüsselung von Daten in Bewegung

Datenverarbeitungsverfahren erfordern die Übertragung vertraulicher und persönlicher Informationen über einen sicheren Kanal. Ein sicherer Kanal ist eine verschlüsselte Netzverbindung.

Es stehen verschiedene Verschlüsselungsmethoden zur Verfügung, die in der Regel in die Anwendung integriert sind. Der Benutzer muss sich darüber im Klaren sein, über welche Datenverbindung sensible Daten übertragen werden und ob die Verschlüsselung für diese Verbindung aktiviert ist.

Verschlüsselung ist erforderlich für

- den Transport sensibler Dateien (Verwendung von SSL oder SCP zur Verschlüsselung sensibler Daten für den Netzzugriff auf unverschlüsselte Dateien).
- Der gesamte Netzwerkverkehr für den Fernzugriff auf die virtuelle Desktop-Umgebung
- Transport sensibler Daten, die Teil einer Datenbankabfrage oder eines Webdienstaufrufs sind (z. B. SQL-Abfrage zum Abrufen oder Senden von Daten aus der Datenbank oder ein Webdienstaufruf zum Abrufen oder Senden von Daten aus einer Cloud-Anwendung).
- Privilegierter Zugang zu Netzwerkgeräten oder Servern zu Zwecken der Systemverwaltung, z. B. SSH

3.13 Bluetooth-Verschlüsselung

Bluetooth ist nicht als Kommunikationsmethode für unverschlüsselte vertrauliche, persönliche oder anderweitig sensible Daten zugelassen.

Siehe die Richtlinien zur Informationsübertragung für die Verwendung von Bluetooth.

4 Einhaltung von Normen

4.1 Messung der Konformität

Das Informationssicherheitsmanagementteam wird die Einhaltung dieser Richtlinie durch verschiedene Methoden überprüfen, einschließlich, aber nicht beschränkt auf Business-Tool-Berichte, interne und externe Audits und Feedback an den Richtlinieninhaber.

4.2 Ausnahmen

Jede Ausnahme von der Richtlinie muss vom Beauftragten für Informationssicherheit im Voraus genehmigt und aufgezeichnet und dem Management Review Team gemeldet werden.

4.3 Nichteinhaltung der Vorschriften

Ein Mitarbeiter, der gegen diese Politik verstoßen hat, kann disziplinarisch belangt werden, was bis zur Entlassung führen kann.

4.4 Kontinuierliche Verbesserung

Diese Politik wird im Rahmen des kontinuierlichen Verbesserungsprozesses aktualisiert und überarbeitet.