Klassifizierung von Informationen Dritter und Spezifikation für den Umgang damit

Einleitung

Nicht alle Informationen fallen unter dieselbe Wertung oder Sensibilität und die Klassifizierung hilft uns dabei, herauszufinden, wie sie zu schützen sind, zeigt unsere Hingabe für diesen Schutz und hilft uns, effizient zu arbeiten.

Wir haben vier Klassifizierungs-Levels:

- Öffentlich
- Intern
- Vertraulich
- Streng vertraulich

Die unten stehende Tabelle bietet einen Leitfaden für die Informationsarten, die in eine der vier Kategorien fallen.

BT-Informationen werden automatisch als vertraulich klassifiziert, sofern nicht anders angegeben.

Wenn Sie nicht sicher sind, in welche Kategorie die Informationen fallen, wenden Sie sich bitte an Ihren BT Security Contact.

Einstufung	Gesamtbeschreibung	Beispiele
Öffentlich – Kat. 1	Öffentliche Informatials auch außerhalb von BT zugänglich.	<ul style="list-style-type: none"> • Werbekampagnen. • Allgemeine Mitteilungen, die bereits frei zugänglich sind (z. B. Pressemitteilungen, öffentliche Artikel über BT) • Öffentlich zugängliche Werbeinformation, wie veröffentlichte Preise oder Angebote
Intern – Kat. 2	<p>BT-Informationen, die für BT-Mitarbeiter und andere Menschen, die Zugang zum Informationsnetzwerk von BT besitzen und dort, wo ein solcher Zugang ein minimales Geschäftsrisiko für BT bedeutet.</p> <p>Interne Informationen könnten der allgemeinen Geheimhaltungspflicht unterliegen (z. B. E-Mails über den normalen Geschäftsbetrieb, Berichte oder Vertragsdokumente), vorausgesetzt diese Informationen sind nicht hinreichend geschäftlich sensibel, um den unten beschriebenen erhöhten Schutz zu benötigen.</p>	<ul style="list-style-type: none"> • Interne Newsletter, wie BT-News • FixIt-Artikel • Allgemeine, nicht sensible E-Mails (z. B. keine Geschäftsinformationen oder eingeschränkten personenbezogenen Daten, wie sie ausführlich in der linken Spalte im Textkörper einer E-Mail vorkommen)
Vertraulich – Kat. 3	Vertrauliche Informationen sind Informationen, die auf ein bestimmtes Publikum beschränkt werden sollten und deren unbefugte Weitergabe den Ruf von BT schädigen könnte oder deren Weitergabe möglicherweise den Menschen schadet, die sie betrifft (z. B. personenbezogene Daten über Angestellte oder Kunden). Das Need-to-know-Prinzip sollte bei vertraulichen	<ul style="list-style-type: none"> • System-Logdaten; • Geschäftlich sensible Verkaufs- und Marketingdaten; • Lokale Geschäftspläne; • Personenbezogene Daten; und • Risikodaten. • Alle personenbezogenen Daten (wie unter der Bedingung „Informationsschutz“ festgelegt), außer sie wurden unten

ÖFFENTLICHES DOKUMENT

	<p>Informationen angewendet werden.</p> <p>Sammlung einiger vertraulicher Dokumente</p> <p>Wenn Sie eine Sammlung „vertraulicher“ Dokumente an einem Ort aufbewahren, könnte eine höhere Einstufung der Klassifizierung nötig werden und dies könnte zu einer erneuten Klassifizierung einzelner Dokumente in die Kategorie „streng vertraulich“ führen oder weitere Sicherheitsmaßnahmen zur Sicherung des Ortes benötigen, wenn:</p> <ul style="list-style-type: none"> • Die Informationen zusammen einen außergewöhnlichen Schaden für BT bedeuten könnten, sollten sie ungewollt veröffentlicht werden; oder • Wenn sie ein attraktives Ziel darstellen, sollten sie in Verbindung mit anderen Daten genutzt werden. 	<p>stehend als streng vertraulich eingestuft.</p>
<p>Streng vertraulich – Kat. 4</p>	<p>Streng vertrauliche Informationen oder Daten werden nur in einem festgelegten und kleinen Umkreis veröffentlicht, das Need-to-know-Prinzip wird genau befolgt (es muss bekannt sein, wer Kopien und wer Zugriff besitzt). Eine unautorisierte Veröffentlichung könnte einen außergewöhnlichen Schaden für BT anrichten. Sie sollten genau abwägen, welche Informationen streng vertraulich sind, da diese die strengsten Sicherheitskontrollen benötigen.</p>	<ul style="list-style-type: none"> • Bankkontodaten • Authentifizierungs-Details sollten als streng vertraulich eingestuft werden. • Computer-Passwörter, Passwörter müssen entsprechend den Kryptographie-Spezifikationen von BT gespeichert und gesichert werden • Daten, die der Embargoprüfung der Finanzbuchhaltung unterliegen, bis zur Veröffentlichung im Jahresbericht • Strategische Geschäftspläne, Wettbewerbsstrategien, neue strategische Produkte und neue Marketingpolitik • Sehr empfindliche Bewertungen von Konkurrenten, Partnern und Vertragsunternehmen • Empfindliche Personal-Informationen, die eine erhebliche Anzahl an Angestellten aufbringen könnten • Details zu großen Geschäftsübernahmen, Verbindungen, Verkäufen und Pläne zu Unternehmenszusammenschlüssen • Details zu erheblichen Netzwerkschwächen • Sicherheitscodes der Kunden, Mastercodes für Verschlüsselungen, Schlüsselberechnungen, Transaktionen, Konto- oder Rechnungsprüfungsinformationen • Prüfberichte oder Berichte über gravierende Defizite/Schwächen bezüglich Praktiken oder Prozesse von BT

Wie gehe ich mit den Daten um?

Die Informationen müssen der Klassifizierung entsprechend gehandhabt werden, damit sie angemessen geschützt sind, unabhängig davon, ob sie sich im Computer oder in einem Netzwerk befinden, geschrieben oder gesprochen sind.

Wir haben Regeln für die Handhabung von Daten und Informationen.

- **Gesprochen und multimedial**, z. B. Gespräche, Aktivität in sozialen Netzwerken, SMS-Mitteilungen, Skype-Gespräche
- **Dokumente auf Papier**, z. B. Ausdrucke, Aushänge, Anordnungen
- **Elektronische Dokumente**, z. B. Sicherungen, E-Mails, Übertragungen, Löschungen
- **In Applikationen oder Systemen**, z. B. Rechenzentren

Wir besitzen außerdem individuelle Richtlinien für das Niveau und die Art der Verschlüsselung, die wir für den Schutz unserer Informationen voraussetzen (unser „Verschlüsselungsstandard“).

Handhabung gesprochener & multimedialer Daten

Ref.	Was möchten Sie tun?	Einstufung	Anforderungen an die Handhabung	Grund
HSM1 0	Ich möchte Informationen in einem sozialen Netzwerk/auf Netzwerk-Seiten veröffentlichen – z. B. auf meinem persönlichen Twitter-Account	Öffentlich	Sie dürfen keine Seiten verlinken oder online Stellungnahmen abgeben, die halbwegs als Meinung von BT verstanden werden könnten oder die gegenüber BT verleumderisch sind und die Marke oder den Ruf von BT Schaden zufügen könnten.	Unautorisierte Veröffentlichungen von Informationen oder persönliche Kommentare könnten unserer Marke schaden
		Intern	Nicht erlaubt	
		Vertraulich	Nicht erlaubt	
		Streng vertraulich	Nicht erlaubt	
HSM2 0	Ich möchte etwas besprechen oder während einer internen Konferenz oder in internen Nachrichten anmerken	Intern	Sie können Live Meeting, WebEx, WebJoin und Lync/Skype for Business nutzen	Interne Daten können von den zum Meeting eingeladenen Personen gesehen werden
		Vertraulich	Sie können Live Meeting, WebEx, WebJoin und Lync/Skype for Business nutzen	Vertrauliche Daten können von den zum Meeting eingeladenen Personen gesehen werden
		Streng vertraulich	<ul style="list-style-type: none"> • Sie können Lync/Skype for Business nutzen, wenn es von BT bereitgestellt wird • Sie müssen die Personen, die an der Konferenz teilnehmen, überprüfen • Sie müssen das Konferenz-Meeting sperren lassen, damit niemand anderes teilnehmen kann 	Lync/Skype for Business ist entsprechend dem Verschlüsselungsstandard verschlüsselt
HSM3 0	Ich möchte etwas über einen externen Live-Chat, z. B. eine Supportseite für Zulieferer wie Cisco, besprechen	Öffentlich	Gespräche müssen auf „öffentliche Informationen“ beschränkt sein, die auf unserer Website frei zugänglich sind	Um eine unbefugte Weitergabe von Informationen zu verhindern
		Intern	Nicht erlaubt	
		Vertraulich	Nicht erlaubt	
		Streng	Nicht erlaubt	

ÖFFENTLICHES DOKUMENT

		vertraulich		
HSM4 0	Ich möchte etwas während eines Videoanrufs/Telefonanrufs besprechen	Intern	Gehen Sie sicher, dass das Gespräch nicht von jemandem mitgehört werden kann, der nicht für BT oder in dessen Auftrag arbeitet	Um eine unautorisierte Veröffentlichung der Informationen zu verhindern
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> Lassen Sie die Identität der Person, mit der Sie sprechen, und deren Need-to-know-Freigabe bestätigen, bevor Sie etwas Vertrauliches besprechen Gehen Sie, wenn möglich, sicher, dass ein Vertrag mit entsprechenden Dritten besteht, bevor Sie das Gespräch beginnen (zu beachten: Bevor Sie Teile oder gesamte Verträge zu einem Dritten zuordnen oder untervergeben, benötigen Sie die vorherige schriftliche Zustimmung von BT) Gehen Sie sicher, dass das Gespräch nicht mitgehört werden kann Hinterlassen Sie keine vertraulichen Informationen auf Voicemail-Systemen 	Um die vertraulichen Informationen zu schützen und sicherzustellen, dass nur diejenigen sie kennen, die sie auch wirklich kennen müssen
		Streng vertraulich	Vgl. „Vertraulich“ und <ul style="list-style-type: none"> Beschränken Sie sich bei streng vertraulichen Informationen auf das absolute Minimum 	
HSM5 0	Ich möchte per SMS/MMS an alle Parteien (intern & extern) eine Nachricht/Inhalte versenden	Öffentlich	Der Inhalt der Nachrichten muss sich auf „öffentliche Informationen“ beschränken, die auf unserer Webseite frei zugänglich sind	Um eine unautorisierte Veröffentlichung der Informationen zu verhindern
		Intern	Keine speziellen Anforderungen an die Handhabung	
		Vertraulich	Gehen Sie sicher, dass die Nachricht nur an diejenigen gesendet wird, die in Kenntnis gesetzt werden müssen und die folgenden Informationen dürfen nicht veröffentlicht werden: <ul style="list-style-type: none"> Kreditkarteninformationen Bankdaten Passwortdetails 	Diese 3 Dinge unterstehen der strengsten Vertraulichkeit
		Streng vertraulich	Nicht erlaubt	

Handhabung von Dokumenten auf Papier

Ref.	Was möchten Sie tun?	Einstufung	Voraussetzungen für die Handhabung	Grund
------	----------------------	------------	------------------------------------	-------

ÖFFENTLICHES DOKUMENT

HPD10	Ich möchte eine ausgedruckte Information in den Geschäftsräumen von Dritten oder zu Hause bearbeiten	Intern	Sie müssen alle Dokumente von Ihrem Schreibtisch entfernen, bevor Sie ihn verlassen	Um eine unbeabsichtigte Veröffentlichung zu vermeiden
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> • Wenn Sie nicht an den Dokumenten arbeiten, nehmen Sie sie beiseite oder schließen Sie sie weg. 	
		Streng vertraulich	Vgl. „Vertraulich“	
HPD20	Ich möchte etwas ausdrucken	Intern	<ul style="list-style-type: none"> • Überprüfen Sie, ob Sie den richtigen Drucker ausgewählt haben • Vergessen Sie keine Dokumente in der Papiaerausgabe 	Um eine unbeabsichtigte Veröffentlichung zu vermeiden
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> • Nutzen Sie einen Drucker, dessen Zugang eingeschränkt ist, einen Drucker, der an einen PC angeschlossen ist oder einen Drucker in einem Raum, dessen Zugang eingeschränkt ist 	
		Streng vertraulich	Vgl. „Vertraulich“	
HPD30	Ich möchte einen Drucker nutzen, der sich weder im Gebäude eines Zulieferers noch in meinem Zuhause befindet (z. B. befindet er sich an einem Standort Dritter, einem Hotel etc.)	Intern	Dies ist normalerweise nicht erlaubt, da Drucker einen Speicher besitzen und Daten abgerufen werden können. Nutzen Sie Ihren gesunden Menschenverstand – möchten Sie wirklich, dass andere diese Informationen sehen?	Daten und Informationen können aus dem Speicher eines Druckers abgerufen werden
		Vertraulich	Nicht erlaubt	
		Streng vertraulich	Nicht erlaubt	
HPD40	Ich möchte Informationen auf Hartkopien außerhalb meines Arbeitsplatzes mitführen	Intern	Führen Sie sie in einem nicht transparenten Ordner oder einer Tasche mit sich	Um sie gegen nicht beabsichtigte Veröffentlichung zu schützen
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> • Sie dürfen keine Kunden- und/oder Zahlungsinformationen aus den Büroräumen von Zulieferern entfernen 	
		Streng vertraulich	Vgl. „Vertraulich“	
HPD50	Ich möchte Informationen auf Hartkopien an interne Parteien verschicken oder sie mit ihnen teilen	Intern	<ul style="list-style-type: none"> • Legen Sie sie in einen Umschlag und verwenden die interne Post. 	Schützen Sie sie vor zufälligen Beobachtern
		Vertraulich	<ul style="list-style-type: none"> • Schreiben Sie nicht „vertraulich“ auf den Umschlag. • Wenn die Informationen dem „Anwaltsgeheimnis“ 	Vermeiden Sie es, zufällige Beobachter darauf aufmerksam zu machen, dass es

ÖFFENTLICHES DOKUMENT

			unterliegen, wenden Sie sich an Ihre Rechtsabteilung.	sich um vertrauliche Informationen handelt. Der Versand per Einschreiben bietet einen Nachweis über die Entsendung, die Unterschrift bei der Lieferung und eine Online-Bestätigung bei der Auslieferung der Sendung					
		Streng vertraulich	<ul style="list-style-type: none"> Nutzen Sie 2 Umschläge und senden Sie sie als nachverfolgbare Lieferung Schreiben Sie nicht „streng vertraulich“ auf den Umschlag Holen Sie die Zustimmung des Besitzers des Dokuments ein, dieses als Hartkopie teilen zu dürfen Übergeben Sie es vorzugsweise persönlich an die berechtigten Personen Ordnen Sie die Kopien durch Wasserzeichen mit einem Namen oder einer Nummer (wenn vorhanden) einzelnen Personen zu Wenn die Dokumente verloren gehen, müssen Sie einen Sicherheitsvorfall melden 	Vermeiden Sie es, zufällige Beobachter darauf aufmerksam zu machen, dass es sich um streng vertrauliche Informationen handelt. Der Versand per Einschreiben bietet einen Nachweis über die Entsendung, die Unterschrift bei der Lieferung und eine Online-Bestätigung bei der Auslieferung der Sendung					
HPD60	Ich möchte Informationen auf Hartkopien an externe Parteien verschicken oder sie mit ihnen teilen	<table border="1"> <tr> <td>Intern</td> <td rowspan="3">Gehen Sie sicher, dass mit den betroffenen Dritten ein Vertrag gemäß HSM40 besteht. In diesem Fall entsprechen die Kontrollmaßnahmen denen für das Teilen von Informationen mit internen Parteien</td> <td rowspan="3">Vgl. HPD50</td> </tr> <tr> <td>Vertraulich</td> </tr> <tr> <td>Streng vertraulich</td> </tr> </table>	Intern	Gehen Sie sicher, dass mit den betroffenen Dritten ein Vertrag gemäß HSM40 besteht. In diesem Fall entsprechen die Kontrollmaßnahmen denen für das Teilen von Informationen mit internen Parteien	Vgl. HPD50	Vertraulich	Streng vertraulich		
Intern	Gehen Sie sicher, dass mit den betroffenen Dritten ein Vertrag gemäß HSM40 besteht. In diesem Fall entsprechen die Kontrollmaßnahmen denen für das Teilen von Informationen mit internen Parteien	Vgl. HPD50							
Vertraulich									
Streng vertraulich									
HPD70	Ich möchte ein Fax senden	<table border="1"> <tr> <td>Intern</td> <td rowspan="3"> <ul style="list-style-type: none"> Sie müssen ein Deckblatt mit einer Testseite schicken und dann den Empfänger für eine Empfangsbestätigung kontaktieren, bevor Sie die Inhaltsseiten faxen Wenn die Informationen dem „Anwaltsgeheimnis“ unterliegen, wenden Sie sich an Ihre Rechtsabteilung </td> <td rowspan="3"> <p>Um eine unbeabsichtigte Veröffentlichung zu vermeiden</p> <p>Um zu verhindern, dass eine unautorisierte Person die Informationen erhält</p> </td> </tr> <tr> <td>Vertraulich</td> </tr> <tr> <td>Streng vertraulich</td> <td>Nicht erlaubt</td> </tr> </table>	Intern	<ul style="list-style-type: none"> Sie müssen ein Deckblatt mit einer Testseite schicken und dann den Empfänger für eine Empfangsbestätigung kontaktieren, bevor Sie die Inhaltsseiten faxen Wenn die Informationen dem „Anwaltsgeheimnis“ unterliegen, wenden Sie sich an Ihre Rechtsabteilung 	<p>Um eine unbeabsichtigte Veröffentlichung zu vermeiden</p> <p>Um zu verhindern, dass eine unautorisierte Person die Informationen erhält</p>	Vertraulich	Streng vertraulich	Nicht erlaubt	
Intern	<ul style="list-style-type: none"> Sie müssen ein Deckblatt mit einer Testseite schicken und dann den Empfänger für eine Empfangsbestätigung kontaktieren, bevor Sie die Inhaltsseiten faxen Wenn die Informationen dem „Anwaltsgeheimnis“ unterliegen, wenden Sie sich an Ihre Rechtsabteilung 	<p>Um eine unbeabsichtigte Veröffentlichung zu vermeiden</p> <p>Um zu verhindern, dass eine unautorisierte Person die Informationen erhält</p>							
Vertraulich									
Streng vertraulich			Nicht erlaubt						
HPD80	Ich möchte Informationen auf Hartkopien vernichten	Intern	<p>Sie müssen</p> <ul style="list-style-type: none"> sie in den Aktenvernichter geben oder in einem Dokumentenmülleimer entsorgen, aus dem die Dokumente nicht einfach entfernt werden können 	Allgemeine Mülleimer und/oder Recycling-Mülleimer sind keine sichere Form der Entsorgung					

ÖFFENTLICHES DOKUMENT

		Vertraulich	Sie müssen die Dokumente auf eine Mindestpartikelgröße von $\leq 160 \text{ mm}^2$ und eine reguläre Partikelstreifenbreite von $\leq 2 \text{ mm}$, z. B. $2 \times 15 \text{ mm}$, zerkleinern.	Um vertrauliche Informationen vor der Veröffentlichung zu schützen
		Streng vertraulich	Sie müssen die Dokumente mit einem Kreuzschnitt-Aktenvernichter auf eine Mindestpartikelgröße von $\leq 160 \text{ mm}^2$ und eine reguläre Partikelstreifenbreite von $\leq 2 \text{ mm}$, z. B. $2 \times 15 \text{ mm}$, zerkleinern.	Um streng vertrauliche Informationen vor der Veröffentlichung zu schützen

Handhabung von elektronischen Dokumenten

Ref.	Was möchten Sie tun?	Einstufung	Anforderungen an die Handhabung	Grund
HED10	Ich möchte elektronische Informationen auf meinem geschäftlichen Laptop/PC speichern	Intern	Umfassende Festplattenverschlüsselung gemäß dem unten genannten Verschlüsselungsstandard.	Dies führt zu einer Verschlüsselung von Informationen in einen nicht lesbaren Code, der nicht auf einfache Weise durch unbefugte Personen entziffert werden kann.
		Vertraulich	Umfassende Festplattenverschlüsselung gemäß dem unten genannten Verschlüsselungsstandard.	
		Streng vertraulich	Umfassende Festplattenverschlüsselung gemäß dem unten genannten Verschlüsselungsstandard.	
HED20	Ich möchte meine Dokumente in SharePoint oder einem anderen Dokumentenmanagement-System speichern, das NICHT in der Cloud oder mit Internet-Dienstleistungen ausgerichtet wird	Intern	<ul style="list-style-type: none"> Nutzen Sie die Zugangs- und Gruppeneinstellungen, um eine rollenbasierte Zugangskontrolle einzurichten. Diese dürfen nicht mehr Zugriff erhalten, als für die Ausführung der Arbeit unbedingt notwendig ist Überprüfen Sie die Zugangskontrolle jedes Jahr 	Beschränkt den Zugang und/oder die Bearbeitungsrechte derer, die im Bilde sein müssen
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> Dokumentieren Sie, welche Personen welcher Rolle zugeteilt werden. Die Rollen und Personen, die diesen zugeteilt wurden, müssen alle 90 Tage überprüft werden Dokumente müssen gemäß dem unten genannten Verschlüsselungsstandard verschlüsselt werden 	
		Streng vertraulich	Vgl. „Intern“ und	

ÖFFENTLICHES DOKUMENT

			<ul style="list-style-type: none"> • Dokumentieren Sie, welche Personen welcher Rolle zugeteilt werden. • Die Rollen und Personen, die diesen zugeteilt wurden, müssen alle 90 Tage überprüft werden • Dokumente müssen gemäß dem unten genannten Verschlüsselungsstandard verschlüsselt werden 	
HED30	Ich möchte elektronische Informationen in der Cloud oder bei Internetdiensten wie Google Docs, GitHub, btcloud.bt.com, Dropbox, Pastebin, Facebook etc. speichern	Intern	Nicht erlaubt	Internet-Dienstleistungen erhöhen das Risiko eines unautorisierten Zugangs zu Informationen
		Vertraulich	Nicht erlaubt	
		Streng vertraulich	Nicht erlaubt	
HED40	Ich möchte elektronische Informationen auf einem Wechseldatenträger, z. B. einem Speicher-Stick, speichern.	Intern	<ul style="list-style-type: none"> • USB-Geräte müssen gemäß dem unten genannten Verschlüsselungsstandard verschlüsselt werden <p>Unter keinen Umständen dürfen personenbezogene Daten auf diesen Geräten gespeichert werden, es sei denn, sie wurden gemäß dem unten genannten Verschlüsselungsstandard verschlüsselt.</p>	Wechseldatenträger können leichter verloren gehen oder gestohlen werden als ein gesamter Computer und deshalb ist das Risiko eines Zugriffs durch nicht berechnete Personen höher. Um Informationen zu schützen, müssen sie in einen unlesbaren Code verschlüsselt werden, der nicht auf einfache Weise durch unbefugte Personen entschlüsselt werden kann
		Vertraulich	Vgl. „Intern“	
		Streng vertraulich	Vgl. „Intern“	
HED50	Ich möchte elektronische Informationen oder Informationen über BT auf meinem privaten Laptop/PC speichern	Intern	Nicht erlaubt	Unbefugte Personen können Zugriff auf BT-Daten erhalten, insbesondere, wenn das Gerät verloren geht, gestohlen wird oder durch ein neueres Modell ersetzt wird.
		Vertraulich	Nicht erlaubt	
		Streng vertraulich	Nicht erlaubt	
HED60	Ich möchte elektronische Informationen oder Dokumente an meine private E-Mail-Adresse senden	Intern	Nicht erlaubt	Um Veröffentlichung für nicht befugte Personen zu vermeiden
		Vertraulich	Nicht erlaubt	
		Streng	Nicht erlaubt	

ÖFFENTLICHES DOKUMENT

		vertraulich		
HED70	Ich möchte Daten automatisch an eine E-Mail-Adresse weiterleiten	Intern	Nicht erlaubt	Unbefugte Personen könnten auf die Daten zugreifen, wenn das E-Mail-Konto, der ISP oder die Internetverbindung beeinträchtigt ist
		Vertraulich	Nicht erlaubt	
		Streng vertraulich	Nicht erlaubt	
HED80	Ich möchte elektronische Informationen <i>intern</i> per E-Mail versenden oder teilen	Intern	Keine speziellen Anforderungen	
		Vertraulich	<ul style="list-style-type: none"> • Machen Sie deutlich, dass es sich um eine vertrauliche E-Mail handelt • Nutzen Sie die Empfindlichkeitseinstellungen, um die E-Mail als vertraulich zu kennzeichnen • Setzen Sie die Zugriffsrechte am besten auf „nicht weiterleiten“ • Wenn die Informationen dem „Anwaltsgeheimnis“ unterliegen, wenden Sie sich an Ihre Rechtsabteilung • 	Um die Kontrolle über vertrauliche Informationen zu behalten
		Streng vertraulich	Vgl. „vertraulich“, plus <ul style="list-style-type: none"> • Nutzen Sie eine sichere E-Mail für das Senden • Wenn eine sichere E-Mail nicht möglich ist, müssen Sie die Datei vor dem Senden gemäß dem unten genannten Verschlüsselungsstandard verschlüsseln • Setzen Sie die Zugriffsrechte auf „nicht weiterleiten“ 	Um die Informationen zu schützen, während Sie sich in den Netzwerken befinden
HED90	Ich möchte elektronische Informationen <i>extern</i> per E-Mail versenden oder teilen	Intern	Sie können nur dann an externe Parteien senden, wenn bereits ein Vertrag gemäß HSM40 besteht	Um die Kontrolle über vertrauliche Informationen zu behalten
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> • Verschlüsseln Sie die Informationen gemäß dem unten genannten Verschlüsselungsstandard • Überprüfen Sie, dass Sie an die richtige E-Mail-Adresse senden • Wenn die Informationen dem „Anwaltsgeheimnis“ unterliegen, wenden Sie sich an Ihre Rechtsabteilung 	
		Streng vertraulich	Vgl. „Vertraulich“	

ÖFFENTLICHES DOKUMENT

HED120	Ich möchte eine Sicherheitskopie elektronischer Dokumente von BT erstellen	Intern	<ul style="list-style-type: none"> Sie müssen Ihre Dokumente gemäß HED030 auf Netzlaufwerken oder auf einem Dokumentenmanagement-System des Zulieferers speichern. Die Sicherheitskopie muss genauso geschützt werden, wie auf dem Netzlaufwerk SharePoint. Wenn Sie Wechseldatenträger verwenden, muss das Gerät gemäß den unten genannten Verschlüsselungsstandards verschlüsselt sein. 	Sicherheitskopien unterliegen derselben Klassifizierung & demselben Schutz wie die Originaldaten
		Vertraulich	Vgl. „Intern“ und <ul style="list-style-type: none"> Verschlüsseln Sie das Dokument gemäß dem unten genannten Verschlüsselungsstandard, bevor Sie eine Sicherheitskopie erstellen 	
		Streng vertraulich	Vgl. „Vertraulich“	

Handhabung von System- und Applikationsdaten

Ref.	Was möchten Sie tun?	Einstufung	Anforderungen an die Handhabung	Grund
HSADE	Ich möchte elektronische Daten & Informationen speichern und aufbereiten, die in einem Datenzentrum gelagert werden oder auf einem Systemserver	Intern	Keine speziellen Anforderungen, wenn alle oben genannten Anforderungen an die Datenspeicherung dieser Einstufung entsprechen.	
		Vertraulich	Sie müssen die Anforderungen an die Datenbereitstellung durch Dritte befolgen http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	
		Streng vertraulich	Vgl. „vertraulich“, plus Um Bankkonten zu schützen, da diese Informationen besonders sensibel sind, sind die folgenden Kontrollen anzuwenden. In dieser Sicherheitsspezifizierung haben diese Kontrollen Vorrang vor allen anderen anwendbaren Kontrollen. 1. Bankkonten müssen für Einzelpersonen in Tokens übersetzt werden (persönliche Bankkonten von	

ÖFFENTLICHES DOKUMENT

			<p>Kunden und BT-Angestellten), darunter auch BT eigene Bankkontodaten und die Bankdaten der zahlreichen BT-Rechtspersonen).</p> <p>2. Wenn eine Applikation lediglich geschäftliche Bankkonten enthält, kann die Drittpartei dafür plädieren (basierend auf Zeit, Kosten, Ressourcen, Anzahl der Konten und Anzahl der Nutzer mit Zugriff auf die Applikation etc.), ob BT zunächst eine auf Verschlüsselung basierende Lösung akzeptiert.</p> <p>Wenn einer auf Verschlüsselung basierten Lösung zugestimmt wird, überprüft BT die Entscheidung, sobald alle Bankkonten geschützt sind und entscheidet, ob es angemessen ist, fortzufahren. Dies wird durch das Risikoniveau und die Risikofreudigkeit des Geschäfts als Ganzes beeinflusst.</p> <p>3. Wenn ein Vertreter im Rahmen eines Geschäftsprozesses (z. B. für die Überprüfung, dass wir im Besitz des richtigen Kontos für die Rechnungsstellung sind, oder während des Kundenkontakts, z. B. per E-Mail, oder auf einer Rechnung) Einsicht in das tatsächliche Bankkonto erhält, dürfen wir lediglich die letzten 4 Ziffern des Bankkontos zeigen (d. h. abgedeckte Bankkontodaten).</p> <p>4. Wenn der Zugriff auf das vollständige Bankkonto benötigt wird (z. B. zur Genehmigung eines Kredits oder einer Lastschrift durch eine Bank), müssen die Bankdaten aus Tokens übersetzt oder die Verschlüsselung aufgehoben werden und dann mit einem verschlüsselten Transportmechanismus entsprechend der BT-Sicherheitspolitik an die Bank weitergeleitet werden. Nachdem die Verschlüsselung aufgehoben oder die Tokens übersetzt wurden, müssen die Bankdaten sofort sicher gelöscht werden.</p>	
--	--	--	---	--

Verschlüsselungsstandards

Allgemeine Kryptographie-Kontrollen.

Ref.	Kontrolle	Grund
C1.10	Es müssen die aktuellen kryptographischen Bibliotheken genutzt werden	Die kryptographischen Bibliotheken werden regelmäßig auf den neuesten Stand gebracht. Zusätzlich zu den Updates der Software-Pakete entsprechend den Anweisungen von Zulieferern sollten die kryptographischen Pakete regelmäßig überprüft und auf den neuesten Stand gebracht werden.
C1.20	Nutzen Sie nur genehmigte Cipher Suites nach Industriestandard zur Verschlüsselung. Z. B. für TLS, SSLv2	Nicht genehmigte Chiffren können zu Schwächen führen
C1.30	Für neue Implementierungen ist die aktuellste Version von TLS zu nutzen. SSL V1, 2 & 3 dürfen nicht genutzt werden	Frühere Versionen bis einschließlich TLS1.0 gelten nicht länger als sicher
C1.40	Die Perfect Forward Secrecy muss gewährleistet sein	Die Algorithmen der Perfect Forward Secrecy verhindern das Entschlüsseln von abgefangenen

ÖFFENTLICHES DOKUMENT

		Nachrichten, auch wenn der private Authentifizierungsschlüssel in Zukunft beeinträchtigt wird
C1.50	Selbst unterzeichnete Bestätigungen sind nicht gestattet	Selbst unterzeichnete Bestätigungen heben den Vorteil einer Endpunktauthentifizierung auf und verringern außerdem die Möglichkeit einer Einzelperson, einen Man-in-the-Middle-Angriff festzustellen.
C1.60 GTS2.370	Eine Zertifizierungsstelle nach Industriestandard muss für die Zertifikatsverwaltung genutzt werden. Z. B. Verisign	Um einen Bestand an Zertifikaten, die für Schwächen und den Ablauf von Zertifikaten ausgestellt wurden, zu haben
C1.70	Passwörter müssen durch eine nicht umkehrbare surjektive mathematische Funktion (z. B. Hash-Algorithmus) mit einer einzigartigen, zufällig gewählten Zeichenfolge (Salt) pro Passwort geschützt werden. NB. SALT sind Zufallsdaten, die genutzt werden, um einer surjektiven Funktion einen zusätzlichen Input zu geben, der ein Passwort oder eine Passphrase zerhackt (engl. to hash).	Gespeicherte Passwortdateien können extrahiert werden und von daher müssen alle Einträge geschützt werden, um die Wiederherstellung von Klartextpasswörtern zu verhindern
C1.80	Geschützte Passwörter gemäß C1.70 müssen getrennt von den Konfigurationsdateien eines Systems gespeichert werden und eine eingebaute Zugriffskontrolle besitzen, damit nur entsprechend berechnete Nutzer die Inhalte lesen oder kopieren können.	Es darf niemals möglich sein, geschützte Passwörter durch Directory Traversal, SNMP Walk, aus dem Konfigurationsdepot oder durch andere Mechanismen abzurufen, was versuchtes Cracking im Offline-Modus zulassen könnte.

Umsetzung der technischen Kryptographie

SSL/TLS Protokolle	
Kann genutzt werden	Darf nicht genutzt werden
TLSv1.3 (Bestätigung folgt – verfügbar für OpenSSL nach dem 5. April).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLSv1.0*	

* TLSv1.0 steht bereits am Ende der Lebensdauer und kann jederzeit aufgrund der bekannten Probleme überholt werden. Aus Gründen der Regelkonformität (zum Beispiel PCI-DSS) müssen Protokolle wie TLSv1.0 und TLSv1.1 möglicherweise abgeschaltet werden. Alle Entwickler sollten darauf eingestellt sein, diese Protokolle durch Konfiguration zu deaktivieren.

Schlüsselgrößen	Schlüsselgrößen		
	Symmetrisch	Asymmetrisch	Elliptische Kurve
Brownfield	≥ 112 Bits	≥ 2048 Bits	≥ 224 Bits
Greenfield	≥ 128 Bits	≥ 3072 Bits	≥ 384 Bits

Schlüsselaustausch	
Kann genutzt werden	Darf nicht genutzt werden
ECDHE (Ephemeral-Diffie-Hellman-Schlüsselaustausch (temporäre Schlüssel) (Schlüssel, die nicht auf Zertifikaten basieren))	kRSA (RSA-Schlüsselaustausch)
	kDhR (Diffie-Hellman-Schlüsselaustausch mit RSA-Schlüssel)
	kDhD (Diffie-Hellman-Schlüsselaustausch mit DSA-Schlüssel)

ÖFFENTLICHES DOKUMENT

	kSRP (Secure-Remote-Password-(SRP)-Schlüsselaustausch)
	kADH (Anonymer Diffie-Hellman-Schlüsselaustausch)
	kPSK (Pre-shared-Key-Schlüsselaustausch)

Die Perfect Forward Secrecy sollte auf lokal konfigurierten oder generierten Diffie-Hellman-Gruppenwerten basieren, die „sichere“ Primzahlen beinhalten.

Diffie-Hellman-Parameter

Diffie-Hellman-Parameter	
Kann genutzt werden	Darf nicht genutzt werden
3072-Bit-Diffie-Hellman-Gruppe (beste – muss lokal generiert werden).	Die Standardwerte des Servers (generieren Sie Ihre eigenen lokal)
2048-Bit-Diffie-Hellman-Gruppe (näher sich Lebensende – muss lokal generiert werden).	

Authentifizierung	
Kann genutzt werden	Darf nicht genutzt werden
aRSA (RSA-Authentifizierung)	aNULL (keine Authentifizierung)
aECDSA (Elliptic-Curve-Digital-Signature-Algorithm-Authentifizierung)	aDSS (DSS-Authentifizierung)
	aECDH (Elliptic Curve Diffie-Hellman)
	aDH (Diffie-Hellman)
	aDSA (Digital Signature Algorithm)
	aPSK (Pre-shared Key)
	aSRP (Secure Remote Password)

Chiffre/Verschlüsselung	
Kann genutzt werden	Darf nicht genutzt werden
AES 256 GCM (Rijndael (Fortgeschrittener Verschlüsselungsstandard) – Galois/Counter Mode)	eNULL (keine Verschlüsselung)
AES 128 GCM (Rijndael (Fortgeschrittener Verschlüsselungsstandard) – Galois/Counter Mode)	DES (DES-Verschlüsselung)
CHACHA20/POLY1305 (256)	3DES (3DES-Verschlüsselung)
AES 256 CCM (Rijndael (Fortgeschrittener Verschlüsselungsstandard) – Counter Mode mit CBC-Mac)	RC4 (RC4-Verschlüsselung)
AES 128 CCM (Rijndael (Fortgeschrittener Verschlüsselungsstandard) – Counter Mode mit CBC-Mac)	RC2 (RC2-Verschlüsselung)
AES 256 CBC (Rijndael Cipher Block Chaining) – nähert sich Lebensende.	IDEA (IDEA-Verschlüsselung)
AES 128 CBC (Rijndael Cipher Block Chaining) – nähert sich Lebensende.	Seed (Seed-Verschlüsselung)
	Camellia (Camellia-Verschlüsselung)
	ARIA (ARIA-Verschlüsselung)

Formatted Table

MAC Digest Algorithm	
Kann genutzt werden	Darf nicht genutzt werden
AEAD (Authenticated Encryption Additional Data)	MD5 (MD5-Hashfunktion)
SHA512 (SHA2-Familie – SHA512-Hashfunktion)	SHA1 (SHA1-Hashfunktion)
SHA384 (SHA2-Familie – SHA384-Hashfunktion)	SHA (Alias für SHA1)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

ÖFFENTLICHES DOKUMENT

SHA256 (SHA2-Familie – SHA256-Hashfunktion)

Formatted: English (United Kingdom)