Bijlage 1 - Informatie classificeren

Inleiding

Binnen BT zijn alle gegevens en informatie in het bezit van een BT-bedrijfseigenaar, die verantwoordelijk is voor de classificatie van het document of de gegevens.

Gegevens en informatie moeten worden beschermd door alle gebruikers die hiermee in aanraking komen. Als gebruiker van BT-informatie bent u verantwoordelijk voor het voldoen aan de veiligheidscontroles van de classificatie in dit document en eventuele specifieke projectvereisten die gespecificeerd worden door BT. U dient alleen het document of de gegevens te gebruiken voor het beoogde doel en u moet toestemming vragen aan de eigenaar van de gegevens, als u meerdere personen toegangsrechten hiervoor wilt verschaffen.

Als u BT-informatie die niet is geclassificeerd ontvangt, moet u contact opnemen met de afzender of uw BT-manager om de classificatie te bevestigen, anders kunt u contact opnemen met BT-veiligheid volgens de Veiligheidseisen in bijlage 3.

N.B. Als u toegang hebt tot de BT Greenside Local Area Network (LAN) of documenten moet aanmaken voor BT die BT- informatie zullen bevatten, dient u het Veiligheidsbeleid 4 te raadplegen, of anders zal het volgende van toepassing zijn

Informatie classificeren

Er zijn 4 manieren om informatie te classificeren:

- Publiek
- Intern
- Vertrouwelijk
- Strikt vertrouwelijk

Publiek

Publieke informatie is niet onderhevig aan controle, en is bedoeld voor publieke consumptie.

Intern

Interne informatie is beschikbaar voor BT-mensen en andere mensen die toegang hebben tot het BT informatienetwerk van BT, en wanneer deze toegang weinig bedrijfsrisico voor BT inhoudt.

Vertrouwelijk

Vertrouwelijke informatie heeft een specifieke doelgroep: het need-to-know principe (toegangscontrole) wordt strikt nageleefd. De ongeoorloofde bekendmaking van Vertrouwelijke informatie kan invloed hebben op de reputatie van BT of mensen schade berokkenen.

Voorbeelden zijn:

- Persoonlijke informatie over individuen, BT-mensen, derden of klanten;
- Systeem-loggegevens;
- Verkoop- en marketinggegevens;

- Lokale bedrijfsplannen;
- Risicogegevens;
- Wachtwoorden.
- Wettelijk vertrouwelijke informatie

Verzamelen van meerdere Vertrouwelijke documenten

Als u meerdere Vertrouwelijke documenten hebt verzameld op één locatie, kan het zijn dat u de classificatie moet upgraden en dit kan leiden tot een nieuwe classificatie van afzonderlijke documenten die Strikt Vertrouwelijk zijn, of er moeten aanvullende veiligheidsmaatregelen worden genomen om de locatie hiervan veilig te stellen:

- Samen kunnen zij uitzonderlijke schade veroorzaken aan BT als deze zouden uitlekken;
- Wanneer deze documenten worden gebruikt in combinatie met andere gegevens bijv. waar persoonsgegevens zoals naam en adres en/of meerdere bankafschriften in een systeem bestaan, zouden deze een aantrekkelijk doelwit vormen.

Als u zich zorgen maakt over de gegevens die u in uw bezit hebt, kunt u contact opnemen met uw contactpersoon bij BT.

Strikt vertrouwelijk

Er zijn slechts een klein aantal strikt Vertrouwelijke informatie of gegevens in omloop; het need-to-know principe strikt wordt streng nageleefd (u moet weten wie kopieën heeft en wie toegang heeft). Ongeoorloofde bekendmaking kan uitzonderlijke schade veroorzaken aan BT. U moet zorgvuldig beoordelen of informatie Strikt Vertrouwelijk is, omdat deze aan de meest strenge veiligheidscontroles onderhevig is.

Veiligheidscontroles

Definities van termen:

Codering

Minimale vereisten:

- Maakt gebruik van AES 256-bits codering.
- Symmetrische sleutels moeten een minimale sleutellengte van 256 bits hebben.
- Asymmetrische sleutels (bijvoorbeeld RSA) moeten een sleutellengte van ten minste 2048 bits hebben.
- Gebruik alleen bekende en vertrouwde cryptografische sleutels.
- Gebruik geen zelf-ondertekende certificaten.

Wachtwoord/Wachtwoordzin – (voor codering)

Mag niet gemakkelijk te raden zijn (d.w.z. moet zo willekeurig mogelijk zijn, geen verband houden met de gebruikers-id, de gebruikers, de identiteit, de datum, enz.), en niet gedetecteerd kunnen worden met behulp van woordenboeken van veelgebruikte wachtwoorden. Ze moeten echter:-

- Minstens 8 tekens lang zijn.
- Minstens twee van de volgende
    - Niet-alfanumerieke tekens bijv. (!, £," $, %,^, &,*, (,), -,_, +, =, :, `, @, ~, #, ?, <,>,)</,> bevatten
    - Decimaal getal: (0... 9)
    - Hoofdletter: (A... Z)

- Persoonlijke sleutels moeten worden beschermd met een wachtwoord met behulp van een combinatie van alfanumerieke tekens en symbolen zoals hierboven gedefinieerd.

NB: Om elke twijfel weg te nemen, zullen alle klantspecifieke contractuele vereisten die in het Contract zijn vervat, en die een hoger veiligheidsniveau vereisen, voorrang hebben op de volgende controles.

	Veiligheidscontroles	Intern	Vertrouwelijk	Strikt vertrouwelijk
1	**Nationale wetgeving voor gegevensbescherming-Persoonsgegevens en gevoelige persoonsgegevens**	Moeten niet als interne gegevens worden behandeld. Beschermen individuele gegevens in de vorm van Vertrouwelijk	Beschermen individuele gegevens in de vorm van Vertrouwelijk	Beschermen bulkgegevens in de vorm van Strikt Vertrouwelijk.
2	**Controles van de verspreiding van zakelijke documenten (Word, Excel) en de tracking hiervan**	Controle en tracking niet vereist. Zet de "**BT-INTERNE**" markering op elke pagina, of "**INTERNE OPENREACH**" als deze alleen in Openreach wordt gedeeld.	Zet "**VERTROUWELIJK**" op elke pagina van het document en verzeker u ervan dat u het "**need to know principe**" volgt, en overweeg het gebruik van een **distributielijst.** **Codering vereist zoals per bovenstaande gedefinieerde begrippen „Coderen" en "**Wachtwoord/Wachtwoordzin**".**	Zet "STRIKT VERTROUWELIJK" op elke pagina van het document. Neem een **distributielijst van** personen in het document op. De eigenaar moet ervoor zorgen dat het "**need to know principe**" wordt gevolgd. **Codering wordt vereist voorafgaand aan opslag, met behulp van software die voldoet aan de bovengenoemde termdefinities „Coderen" en "**Wachtwoord/Wachtwoordzin**", indien** gegevens niet op een door BT geleverde PC/Laptop met harde schijf-codering, d.w.z. verwijderbare media worden opgeslagen. Hetzelfde geldt wanneer u e-mailt

				naar iemand, of dit een persoon is van BT of niet.
3	**Veilige opslag op: laptop en PC**	Veilige opslag wordt vereist, bijvoorbeeld PGP, WinZip 9.	Hele disk-codering **zoals per bovenstaande termdefinities "Coderen" en "**Wachtwoord/Wachtwoordzin**".**	Hele disk-codering **zoals per bovenstaande termdefinities "Coderen" en "**Wachtwoord/Wachtwoordzin**".**
4	**Veilige opslag op de server en gegevensbestanden (vaste - schijf/tape)**	Veilige opslag niet vereist, indien deze voldoet aan alle fysieke eisen, anders wordt veilige opslag vereist, bijv. PGP, WinZip 9	BT-informatie moet gecodeerd zijn "**zoals per bovenstaande termdefinities "Coderen" en "**Wachtwoord/Wachtwoordzin**".**	**BT-informatie moet gecodeerd zijn "**zoals per bovenstaande termdefinities "Coderen" en "Wachtwoord/Wachtwoordzin".**
5	**Veilige opslag op Blackberry, Windows Mobile, andere PDA's, tabletten (iPads etc.), mobiele telefoons en MP3-spelers**	Het is verboden om Interne informatie op dergelijke apparaten op te slaan, tenzij het apparaat is geleverd door BT of een licentie heeft die is goedgekeurd door BT-Veiligheid. Dergelijke apparaten moeten niet worden geconfigureerd voor de toegang tot BMT.com e-mailaccounts (toegang tot bt.com e-mail via webmail is toegestaan).	Het is verboden om Vertrouwelijke informatie op dergelijke apparatuur op te slaan, tenzij het apparaat is geleverd door BT of een licentie heeft die is goedgekeurd door BT-veiligheid. Dergelijke apparaten moeten niet worden geconfigureerd voor de toegang tot BMT.com e-mailaccounts (toegang tot bt.com e-mail via webmail is toegestaan).	Het is verboden om ISC op te slaan op dergelijke apparaten.
6	**Veilige opslag op:** **Verwijderbare media zoals geheugenstick, flash geheugen, cd/dvd, USB-harde schijven, veilige digitale kaarten, diskettes en andere gelijksoortige apparaten.**	BT-informatie moet gecodeerd zijn, als deze op dergelijke apparatuur wordt opgeslagen "**zoals per bovenstaande termdefinities "Coderen" en** Wachtwoord/Wachtwoordzin**"**	**BT-informatie moet gecodeerd zijn, als deze op dergelijke apparatuur wordt opgeslagen "**zoals per bovenstaande termdefinities "Coderen" en "Wachtwoord/Wachtwoordzin".	Het is verboden om ISC op te slaan op dergelijke apparaten.

7	**Web/on-line opslag of een Internet opslagfaciliteit**	Verboden	Verboden	Verboden
8	**Externe samenwerking op het Web**	Elk MS LiveMeeting platform of Webjoin	Verboden	Verboden
9	**Verstuurd via e-mail**	Codering is niet vereist.	Gecodeerd voor geadresseerden (waar de bestemming niet bt.com e-mail is) per bovenstaande termdefinities "Coderen" en ""Wachtwoord/Wachtwoordzin".	**Codering vereist zoals per bovenstaande gedefinieerde begrippen „Coderen" en "**Wachtwoord/Wachtwoordzin**".**
10	**Automatisch doorsturen van e-mail**	Verboden	Verboden	Verboden
11	**Netwerktransmissie**	Codering is niet vereist.	Gecodeerd voor externe en interne transmissies, **per bovenstaande termdefinities „Coderen" en ""**Wachtwoord/Wachtwoordzin".	Gecodeerd voor externe en interne transmissies, **per bovenstaande termdefinities „Coderen" en ""**Wachtwoord/Wachtwoordzin".
12	**Bestandsoverdracht**	Beveiligde bestandsoverdracht gebruiken, bijv. SFTP, XFB.	Beveiligde bestandsoverdracht gebruiken, bijv. SFTP, XFB.	Beveiligde bestandsoverdracht gebruiken, bijv. SFTP, XFB.
13	**Gegevens wissen/verwijderen**	Toepassing of uitwisfaciliteiten van besturingssysteem gebruiken.	Gegevens saneren door elke sector ten minste eenmaal te overschrijven met willekeurige binaire strings, met behulp van een softwareproduct bijvoorbeeld Blanco HMG Edition of Blanco versie 5 als u Solid State apparaten gebruikt.	Gegevens saneren door elke sector minstens eenmaal te overschrijven met willekeurige binaire strings, met behulp van een softwareproduct, zoals Blanco HMG Edition of Blanco versie 5 als u Solid State-apparaten gebruikt.
14	**Verwijdering of hergebruik van IT-apparatuur (die BT-informatie bevat)**	Gebruik bij het wissen een controleerbare en geteste software-oplossing, waarbij een officieel certificaat wordt gegeven, om te	Schijven (of andere opslagmedia, met inbegrip van maar niet beperkt tot compact flash en solid state-apparatuur) moeten worden gesaneerd door elke sector ten	Schijven (of andere opslagmedia, met inbegrip van maar niet beperkt tot compact flash en solid state-apparatuur) moeten worden gesaneerd door elke sector ten

	Met inbegrip van maar niet beperkt tot: **- Verwijdering van onderdelen** **- Vernietiging van leveranciersapparatuur** **- Vernietigingseisen voor back-ups** **- Serveronderdelen die worden teruggestuurd naar de fabrikant voor reparatie**	verzekeren dat het wissen geslaagd is. Alle apparatuur die er niet in slaagt om te wissen moet worden vernietigd, waarvoor een officieel certificaat moeten worden ontvangen/geleverd, met ten minste een lijst van de serienummers van de apparatuur, als bewijs van de verwijdering. De bovenstaande oplossing kan niet worden gebruikt met Solid State Drive (SSD's) die moeten worden vernietigd en waarvoor officiële certificering wordt ontvangen/geleverd. Zie BSD-EN 17513 voor meer informatie.	minste eenmaal te overschrijven met willekeurige binaire strings, met behulp van een softwareproduct bijvoorbeeld Blanco HMG Edition of Blanco versie 5 als u Solid State apparaten gebruikt. Als sanering niet haalbaar is of niet van toepassing, dan moet de schijf (of andere opslagmiddelen met inbegrip van maar niet beperkt tot compact flash, solid state-apparatuur) worden vernietigd met behulp van een faciliteit voor het vernietigen van schijven. Een formeel certificaat moet worden geproduceerd om de uitwissing of vernietiging te controleren.	minste eenmaal te overschrijven met willekeurige binaire strings, met behulp van een softwareproduct bijvoorbeeld Blanco HMG Edition of Blanco versie 5 als u Solid State apparaten gebruikt. Als sanering niet haalbaar is of niet van toepassing, dan moet de schijf (of andere opslagmiddelen met inbegrip van maar niet beperkt tot compact flash, solid state-apparatuur) worden vernietigd met behulp van een faciliteit voor het vernietigen van schijven. Een formeel certificaat moet worden geproduceerd om de uitwissing of vernietiging te controleren.
15	**Afdrukken**	Gebruik een printer aangesloten op de pc of op een netwerkprinter waarbij u aanwezig moet zijn tijdens het afdrukken.	Gebruik een PIN-gecontroleerde printer of printer aangesloten op de pc, oftewel een printer in een kamer met toegangsbeheer. Controleer om welke printer het gaat en geen documenten in de printlade achterlaten.	Gebruik een PIN-gecontroleerde printer of printer aangesloten op de pc, oftewel een printer in een kamer met toegangsbeheer. Wees voorzichtig wanneer u afdrukt. Controleer om welke printer het gaat en geen documenten in de printlade achterlaten.
16	**Post/koeriersdiensten tussen BT en de Leverancier**	Enkele envelop.	Gebruik dubbele enveloppen en aangetekend verzenden aan de geadresseerde alleen, en zet niet "Vertrouwelijk" op de 1e envelop.	Gebruik dubbele enveloppen en aangetekend verzenden aan de geadresseerde alleen, en zet niet "Strikt Vertrouwelijk" op de 1e envelop.

17	**Externe openbaarmaking**	Toestemming aan BT-Veiligheidspartner vragen Zie bijlage 3.	Toestemming aan BT-Veiligheidspartner vragen Zie bijlage 3.	Toestemming aan BT-Veiligheidspartner vragen Zie bijlage 3.
18	**Gebruikt voor training, ontwikkeling of testen**	Moeten anoniem wordt gemaakt door BT en voldoen aan de beste praktijken van het anoniem maken van BT-gegevens, volgens handleiding BP001.	Moeten anoniem wordt gemaakt door BT en voldoen aan de beste praktijken van het anoniem maken van BT-gegevens, volgens handleiding BP001.	Verboden
19	**Verwijderen van papier**	Versnipperd met behulp van cross cut-versnipperaars.	Versnipperd met behulp van cross cut-versnipperaars.	Versnipperd met behulp van cross cut-versnipperaars, tot een afmeting van 4 x 15 mm.
20	**Openbare ruimtes**	Niet praten over Interne informatie in het openbaar.	Niet praten over Vertrouwelijke informatie in het openbaar. Niet werken aan documenten in openbare ruimtes, waar personen mee kunnen kijken.	Niet praten over Strikt Vertrouwelijke informatie in het openbaar. Niet werken aan documenten in openbare ruimtes