Allegato 1 Classificazione delle informazioni

Introduzione

Nell'organizzazione BT, tutti i dati e tutte le informazioni hanno un proprietario aziendale responsabile della loro classificazione.

I dati e le informazioni devono essere protetti da tutti gli utenti che entrano in contatto con essi. Ogni utente delle informazioni BT è responsabile dell'osservanza dei controlli relativi alla classificazione della sicurezza enunciati in questo documento nonché dei requisiti validi per progetti specifici prescritti da BT. L'utilizzo del documento o dei dati deve essere circoscritto alle finalità previste e per consentirne l'accesso ad altre persone sarà necessario ottenere l'approvazione del proprietario dei dati.

Qualora si ricevano informazioni BT non classificate, sarà necessario contattare il mittente o il proprio responsabile BT per una verifica della classificazione, oppure rivolgersi a BT Security come da allegato 3 dei requisiti di sicurezza.

N.B. Se si dispone dell'accesso alla rete locale (LAN) di BT Greenside o si è tenuti a creare documenti per BT contenenti informazioni BT, sarà necessario fare riferimento alla Politica di sicurezza 4. In caso contrario sarà applicabile quanto segue.

Classificazione delle informazioni

Le informazioni possono essere classificate secondo 4 diverse tipologie:

- Pubbliche
- Per uso interno
- Riservate
- Strettamente riservate

Pubbliche

Le informazioni pubbliche non richiedono alcun controllo, essendo destinate ad una fruizione pubblica.

Per uso interno

Le informazioni per uso interno sono a disposizione del personale BT e di altri addetti che possono accedere alla rete informatica di BT a condizione che tale accesso comporti un rischio aziendale di scarsa rilevanza per BT.

Riservate

Le informazioni riservate sono rivolte a destinatari specifici e sono rigorosamente disciplinate dal principio della necessità di sapere (controlli dell'accesso). La divulgazione non autorizzata delle informazioni riservate potrebbe compromettere la reputazione di BT o comportare un pericolo per le persone.

Sono incluse in questa categoria:

- informazioni personali su singoli individui, siano essi membri del personale di BT, terzi o clienti;
- dati del registro di sistema;

- dati relativi a vendite e marketing;
- piani aziendali locali;
- dati relativi ai rischi;
- password;
- informazioni riservate per obbligo di legge.

Raccolta di molteplici documenti riservati

La presenza di una raccolta di documenti Riservati presso la stessa sede può comportare l'obbligo di rivederne la classificazione. Ciò potrebbe determinare la riclassificazione di singoli documenti come strettamente riservati o richiedere l'introduzione di ulteriori misure di sicurezza per rendere idonea la sede se:

- complessivamente, sono tali da recare un danno a BT qualora venissero dispersi;
- quando utilizzati con altre combinazioni di dati, ad esempio, nome e indirizzo e/o quando in un sistema sono presenti molteplici registrazioni di estremi bancari, potrebbero diventare un bersaglio ambito.

In caso di dubbi circa le informazioni in proprio possesso, rivolgersi al referente BT.

Strettamente riservate

I dati o le informazioni strettamente riservati si caratterizzano per una diffusione circoscritta e destinata a un numero limitato di soggetti e sono rigorosamente disciplinati dal principio della necessità di sapere (è necessario sapere chi ne possiede copie e chi può accedervi). La divulgazione non autorizzata potrebbe recare un danno eccezionale a BT. Le informazioni strettamente riservate richiedono i controlli di sicurezza più severi e pertanto l'utente è tenuto a valutarne attentamente la natura.

Controlli di sicurezza

Definizione dei termini:

Crittografia

Requisiti minimi:

- Utilizzare la crittografia AES a 256 bit.
- Le chiavi simmetriche devono avere una lunghezza minima di 256 bit.
- Le chiavi asimmetriche (ad esempio RSA) devono avere una lunghezza minima di 2048 bit.
- Utilizzare unicamente cifrari crittografici noti e attendibili.
- Non utilizzare certificati autofirmati.

Password/Passphrase – (per crittografia)

Non devono essere facilmente intuibili (ad esempio, devono essere il più possibile casuali e non fare riferimento a ID utenti, nomi utenti, identità, date, ecc.), e non essere riconoscibili utilizzando dizionari di password di uso comune. Tuttavia, come requisiti minimi devono:

- avere una lunghezza minima di 8 caratteri;
- contenere almeno due dei seguenti caratteri:
  - caratteri non alfanumerici, ad es. (!, £,", $, %,^, &,*, (,), -,_, +, =, :, `, @, ~, #, ?, <, >,);
  - numeri decimali: (0... 9)
  - lettere maiuscole: (A... Z).
- Le chiavi private devono essere protette con una passphrase formata da una combinazione di caratteri alfanumerici e simboli, come indicato sopra.

NB: per chiarezza, si precisa che qualsiasi requisito contrattuale specifico contenuto in un contratto del cliente che richieda un livello di sicurezza più elevato dovrà prevalere sui controlli riportati di seguito.

	Controlli di sicurezza	Per uso interno	Riservato	Strettamente riservato
1	**Legislazione nazionale sulla protezione dei dati - Dati personali e dati personali sensibili**	Non devono essere trattati come dati per uso interno. Proteggere i registri individuali come documenti riservati.	Proteggere i registri individuali come documenti riservati.	Proteggere i registri collettivi come documenti strettamente riservati.

2	**Controllo della distribuzione e tracciamento dei movimenti dei documenti aziendali (Word, Excel, ecc.)**	Controllo e tracciamento non obbligatori. Inserire la dicitura "**PER USO INTERNO BT**" in ogni pagina o "**PER USO INTERNO OPENREACH**" se il documento deve essere condiviso solo in Openreach.	Inserire la dicitura "**RISERVATO**" in ogni pagina del documento e assicurarsi di aderire al "**principio della necessità di sapere**", valutando peraltro il ricorso ad un **elenco di distribuzione**. Crittografia obbligatoria come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	Inserire la dicitura "STRETTAMENTE RISERVATO" in ogni pagina del documento. Includere un **elenco di distribuzione** di persone nel documento. Il proprietario deve accertarsi che venga rispettato il "**principio della necessità di sapere**". Crittografia obbligatoria prima dell'archiviazione mediante software conforme alla definizione dei termini "crittografia" e "password/passphrase" di cui sopra quando i dati non vengono archiviati in un computer fisso o portatile fornito da BT con crittografia del disco rigido, ossia supporti rimovibili. La stessa regola si applica all'invio di e-mail a qualsiasi destinatario (BT o non BT).
3	**Archiviazione sicura su computer fisso e portatile**	L'archiviazione sicura è obbligatoria (ad es. PGP, WinZip 9).	Crittografia dell'intero disco come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	Crittografia dell'intero disco come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.
4	**Archiviazione sicura su server e database (fisso - disco/nastro)**	Archiviazione sicura non è richiesta se conforme a tutti i requisiti di sicurezza fisica di ; in caso contrario, l'archiviazione sicura è obbligatoria (ad es. PGP, WinZip 9).	Le informazioni BT devono essere crittografate come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	Le informazioni BT devono essere crittografate come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.

5	**Archiviazione sicura su Blackberry, Windows Mobile, altri smartphone, tablet (iPad, ecc.), telefoni cellulari e lettori MP3**	È vietato archiviare informazioni per uso interno su tali dispositivi a meno che il dispositivo venga fornito da BT o che una deroga venga approvata da BT Security. Tali dispositivi non devono essere configurati per l'accesso agli account e-mail BT.com, mentre è consentito l'accesso all'e-mail bt.com tramite webmail.	È vietato archiviare informazioni riservate su tali dispositivi a meno che il dispositivo venga fornito da BT o che una deroga venga approvata da BT Security. Tali dispositivi non devono essere configurati per l'accesso agli account e-mail BT.com, mentre è consentito l'accesso all'e-mail bt.com tramite webmail.	È vietato archiviare informazioni strettamente riservate su tali dispositivi.
6	**Archiviazione sicura su:** **supporti rimovibili quali chiavette USB, memoria flash, CD/DVD, dischi rigidi USB, schede Secure Digital, floppy disk e altri dispositivi similari.**	Se archiviate su tali dispositivi, le informazioni BT devono essere crittografate come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	Se archiviate su tali dispositivi, le informazioni BT devono essere crittografate come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	È vietato archiviare informazioni strettamente riservate su tali dispositivi.
7	**Archiviazione online/su Web o altro servizio di archiviazione tramite Internet**	Vietata	Vietata	Vietata
8	**Collaborazione esterna su Web**	Qualsiasi piattaforma MS LiveMeeting o Webjoin	Vietata	Vietata
9	**Invio tramite e-mail**	Crittografia non obbligatoria.	Informazioni crittografate per i destinatari non bt.com, come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	Crittografia obbligatoria come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.
10	**Inoltro automatico di e-mail**	Vietato	Vietato	Vietato

11	**Trasmissione in rete**	Crittografia non obbligatoria.	Informazioni crittografate per trasmissione esterna e interna, come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.	Informazioni crittografate per trasmissione esterna e interna, come da definizione dei termini "crittografia" e "password/passphrase" di cui sopra.
12	**Trasferimento di file**	Utilizzare un sistema di trasferimento file sicuro, ad es. SFTP, XFB.	Utilizzare un sistema di trasferimento file sicuro, ad es. SFTP, XFB.	Utilizzare un sistema di trasferimento file sicuro, ad es. SFTP, XFB.
13	**Cancellazione/eliminazione di dati**	Utilizzare gli strumenti di eliminazione dati delle applicazioni o del sistema operativo.	Purificare i dati sovrascrivendo ciascun settore con stringhe binarie casuali mediante un software apposito, ad es. Blanco edizione HMG o Blanco versione 5 se si utilizzano dispositivi a stato solido.	Purificare i dati sovrascrivendo ciascun settore con stringhe binarie casuali mediante un software apposito, ad es. Blanco edizione HMG o Blanco versione 5 se si utilizzano dispositivi a stato solido.
14	**Smaltimento o riutilizzo di apparecchiature IT (contenenti informazioni BT)** **Riguarda, senza intento limitativo:** **- Smaltimento di componenti** **- Distruzione di apparecchiature del fornitore** **- Requisiti di distruzione per backup** **- Parti di server rispedite al produttore per la riparazione**	Utilizzare una soluzione software di cancellazione verificabile e testata quando viene prodotto un certificato formale di verifica della cancellazione. Le apparecchiature in cui la cancellazione non riesca devono essere distrutte e una certificazione formale deve essere ricevuta/fornita con almeno la registrazione del numero di serie dell'apparecchiatura come prova dello smaltimento. La soluzione di cui sopra non può essere utilizzata con i dispositivi a stato solido (SSD) che devono essere distrutti e	I dischi (o altri supporti di archiviazione, inclusi, senza intento limitativo, i dispositivi a stato solido e le memorie flash) devono essere purificati sovrascrivendo ciascun settore con stringhe binarie casuali mediante un software apposito, ad es. Blanco edizione HMG o Blanco versione 5 se si utilizzano dispositivi a stato solido. Se la purificazione non può essere effettuata o non è appropriata, il disco (o altro supporto di archiviazione, inclusi, senza intento limitativo, i dispositivi a stato solido e le memorie flash) deve essere distrutto inviandolo presso un centro apposito.	I dischi (o altri supporti di archiviazione, inclusi, senza intento limitativo, i dispositivi a stato solido e le memorie flash) devono essere purificati sovrascrivendo ciascun settore con stringhe binarie casuali mediante un software apposito, ad es. Blanco edizione HMG o Blanco versione 5 se si utilizzano dispositivi a stato solido. Se la purificazione non può essere effettuata o non è appropriata, il disco (o altro supporto di archiviazione, inclusi, senza intento limitativo, i dispositivi a stato solido e le memorie flash) deve essere distrutto inviandolo presso un centro apposito.

		quando deve essere ricevuta/fornita una certificazione formale. Per ulteriori informazioni fare riferimento alla norma BS EN 17513.	Una certificazione formale deve essere prodotta a riprova dell'avvenuta cancellazione o distruzione.	Una certificazione formale deve essere prodotta a riprova dell'avvenuta cancellazione o distruzione.
15	**Stampa**	Utilizzare una stampante collegata al PC o una stampante di rete, portandosi nei pressi della stessa durante la stampa.	Utilizzare una stampante controllata mediante PIN, una stampante collegata al PC o una stampante presente in una stanza ad accesso controllato. Verificare attentamente la stampante a cui vengono inviati i dati e non lasciare documenti nel vassoio.	Utilizzare una stampante controllata mediante PIN, una stampante collegata al PC o una stampante presente in una stanza ad accesso controllato. Prestare attenzione durante la stampa. Verificare attentamente la stampante a cui vengono inviati i dati e non lasciare documenti nel vassoio.
16	**Servizio postale/corriere tra BT e il Fornitore**	Busta singola.	Utilizzare la doppia busta e inviare a mezzo lettera raccomandata unicamente al destinatario e non apporre la dicitura "riservato" sulla 1ª busta.	Utilizzare la doppia busta e inviare a mezzo lettera raccomandata unicamente al destinatario e non apporre la dicitura "strettamente riservato" sulla 1ª busta.
17	**Divulgazione esterna**	Chiedere l'autorizzazione del referente di BT Security. Fare riferimento all'allegato 3.	Chiedere l'autorizzazione del referente di BT Security. Fare riferimento all'allegato 3.	Chiedere l'autorizzazione del referente di BT Security. Fare riferimento all'allegato 3.
18	**Utilizzo in attività di formazione, sviluppo e test**	Le informazioni devono essere rese in forma anonima da BT e aderire alla guida BT sulle migliori prassi di anonimizzazione dei dati (BP001).	Le informazioni devono essere rese in forma anonima da BT e aderire alla guida BT sulle migliori prassi di anonimizzazione dei dati (BP001).	Vietato

19	**Smaltimento di supporti cartacei**	Distruzione mediante macchina distruggi-documenti.	Distruzione mediante macchina distruggi-documenti.	Distruzione in particelle da 4 x 15 mm mediante macchina distruggi-documenti.
20	**Aree pubbliche**	Non parlare di informazioni per uso interno in pubblico.	Non parlare di informazioni riservate in pubblico. Non lavorare su documenti in spazi pubblici in cui si potrebbe essere osservati.	Non parlare di informazioni strettamente riservate in pubblico. Non lavorare sui documenti in spazi pubblici.