

## **1. Impegni di BBBell**

BBBell ha sempre svolto le sue attività in ottica di Sicurezza; per questo motivo ha deciso di certificarsi in base alla Norma Internazionale ISO/IEC 27001:2013 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni) e successivamente con l'estensione all'applicazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

BBBell considera il citato Sistema uno strumento strategico attraverso il quale perseguire la soddisfazione del Cliente e i propri obiettivi di sviluppo e di business.

L'azienda si propone di rimanere all'avanguardia nel processo evolutivo del mercato delle Telecomunicazioni, aggiornando costantemente la propria offerta e i propri sistemi.

La mancanza di adeguati livelli di sicurezza può influire sulla reputazione aziendale, la violazione di impegni contrattuali con il cliente e violazione delle normative vigenti che possono generare ingenti danni di natura economica e finanziaria.

Per questi motivi, BBBell promuove tutte le azioni necessarie affinché i processi e le attività siano orientati al raggiungimento dei seguenti obiettivi:

- Identificare le esigenze di sicurezza tramite l'analisi dei rischi al fine di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo.
- Attuare le azioni necessarie per mitigare i rischi individuati e le misure di sicurezza più idonee.
- Garantire la massima sicurezza delle informazioni dei clienti, in termini di riservatezza, disponibilità e integrità delle informazioni stesse fornendo così un servizio ad alto valore aggiunto.
- Dare continuità operativa ai servizi critici anche a seguito di gravi incidenti.
- Tutelare i diritti e gli interessi di tutti coloro che interagiscono con l'azienda (clienti, dipendenti, collaboratori, terze parti, ecc..).
- Salvaguardare gli interessi degli investitori e dei partners.
- Garantire un livello di servizio eccellente.

## **2. Impegni del Fornitore**

BBBell per garantire ai propri Clienti elevati standard di sicurezza delle informazioni richiede ai propri fornitori di assicurare:

- ✓ La riservatezza delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- ✓ L'integrità delle informazioni: ovvero proteggere le informazioni da modifiche non autorizzate o non previste.
- ✓ La disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni collegate nel momento in cui lo richiedono.

Al tal fine, il fornitore dovrà attenersi ai principi generali nella gestione della sicurezza delle informazioni di seguito esposti:

- ogni accesso ai sistemi di BBBell è sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e sono periodicamente sottoposte a revisione.
- Devono essere rispettate le procedure in essere per l'utilizzo sicuro dei beni aziendali, delle informazioni e dei loro sistemi di gestione; in particolare, relativamente ad eventuali dispositivi consegnati per il loro utilizzo (p.e. tablet):
  - L'utente è responsabile del dispositivo assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
  - Deve essere posta particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
  - In caso di allontanamento, non devono essere abbandonati, ma custoditi in un luogo protetto
  - Sul disco interno devono essere conservati solo i files strettamente necessari.
  - Nel caso di accesso alla rete aziendale tramite Accesso da Remoto: utilizzare l'accesso in forma esclusivamente personale, utilizzare la password non divulgandola a terzi, compresi i membri del nucleo familiare
  - Disconnettersi dal sistema di Accesso Remoto al termine della sessione di lavoro.
  - Non utilizzare abbonamenti Internet privati e non utilizzare i dispositivi per scopi personali.
  - Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul PC assegnatogli, salvo previa richiesta all'ADS (Amministratore di Sistema) che chiederà preventiva autorizzazione alla Direzione.

- Nel caso di furto o smarrimento del dispositivo deve essere data immediata comunicazione all'ADS (Amministratore di Sistema) per l'attuazione delle procedure di cancellazione da remoto, nel caso sia necessario per il livello delle informazioni contenute, ed eventuali notifiche agli Enti preposti.
- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni verso tutto il personale (dipendenti, collaboratori e altri aventi titolo) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- Per poter gestire in modo tempestivo gli incidenti, relativi alla Sicurezza delle Informazioni, il Fornitore deve notificare tempestivamente qualsiasi problema relativo alla sicurezza.
- Non può accedere, senza autorizzazione, alle sedi e ai singoli locali aziendali dove sono gestite le informazioni al fine di garantire la sicurezza delle apparecchiature.
- Deve impegnarsi ad assicurare la conformità ai requisiti legali e ai principi legati alla sicurezza delle informazioni nei rapporti con BBBell e i suoi clienti.
- Deve predisporre tutte le azioni idonee ad affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sul servizio erogato a e da BBBell.
- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi relative all'attività svolta dal fornitore.
- Deve garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Il Fornitore che, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

### **3. Trattamento dei dati personali a norma del GDPR 679/2016 e s.m.i.**

#### **3.1 Istruzioni generali sul trattamento dei dati**

Al fine di assicurare che il trattamento venga effettuato nel pieno rispetto delle norme vigenti, si rammenta il disposto dell'art. 5 GDPR 679/2016, cioè che i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e se necessario aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservati in una forma che consenta l'identificazione per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati.

#### **3.2 Modalità operative da seguire per il trattamento dei dati**

Al fine di effettuare correttamente i trattamenti oggetto di comunicazione da parte di BBBell S.p.A., il Fornitore deve attenersi alle indicazioni che seguono:

- custodire i dati oggetto di trattamento in luoghi non accessibili a soggetti non autorizzati;
- non lasciare incustoditi e accessibili a terzi gli strumenti di lavoro;
- procedere alla sistematica archiviazione dei supporti cartacei e dei digitali nei luoghi a ciò predisposti;
- custodire con attenzione e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici.

#### **3.3 Limiti di effettuazione dei trattamenti consentiti**

In ogni caso, il Fornitore dovrà rispettare in modo rigoroso i seguenti limiti:

- ✓ non potrà, senza preventiva autorizzazione, utilizzare in modo diverso da quanto in precedenza indicato i dati oggetto di comunicazione;
- ✓ non dovrà comunicare a terzi i dati a lei comunicati;
- ✓ dovrà conservare i supporti e gli strumenti contenenti i dati personali in modo da evitare che siano accessibili a persone non autorizzate;
- ✓ ogni comunicazione di dati verso l'esterno, che non sia prevista dalla prestazione affidata, dovrà essere autorizzata preventivamente da BBBell quale Titolare del Trattamento;

I divieti di comunicazione e di diffusione summenzionati, permangono anche dopo la conclusione del contratto in essere.

### 3.4 Riservatezza

Infine, il Fornitore dovrà mantenere durante lo svolgimento del mandato e anche dopo la sua conclusione, la totale riservatezza su tutte le informazioni, siano esse confidenziali e/o riservate di cui è venuto a conoscenza. Dette informazioni non dovranno essere divulgate a terzi, né in tutto né in parte, né in forma scritta o orale o grafica o su supporto magnetico o in qualsiasi altra forma senza la preventiva espressa autorizzazione del Titolare del trattamento.

Per "informazione confidenziale e/o riservata" si intende qualsiasi informazione, dato, disegno, conoscenza, ritrovato, brevettato o brevettabile, know-how e, in genere, qualsivoglia notizia, di natura tecnica, economica, commerciale o amministrativa, così come qualsiasi disegno, documento, supporto magnetico o campione di materiale o prodotto contrassegnato con la dicitura "riservato" o "confidenziale" o comunque, seppur non contrassegnato, ma identificato anche oralmente come tale dal Titolare del trattamento, che lo comunica al fornitore del servizio in relazione all'adempimento del suo mandato.