DISPOSIZIONI ICT

Dipartimento: Legal & Compliance

Autore: Christina Hooker Legal Counsel

Creato: Berna, 07.06.2021

Il presente regolamento disciplina la modalità di impiego degli strumenti informatici e delle informazioni delle aziende di BMS. Un uso non conforme degli strumenti informatici espone BMS a molteplici rischi, tra cui virus informatici, la compromissione della disponibilità di sistemi e servizi nonché conseguenze legali. Il contributo di tutte le collaboratrici
e di tutti i collaboratori è essenziale per il raggiungimento di un adeguato livello di sicurezza.

Ambito di validità

Le presenti disposizioni ai applicano a tutti i collaboratori delle aziende di BMS, che sono:

- BR Bauhandel AG
- Gétaz-Miauton SA
- Barrit Baubedarf AG
- Regusci Reco SA

Le presenti disposizioni sono allegate al regolamento del personale. BMS ha facoltà di integrare e modificare il presente regolamento in qualsiasi momento. La versione delle disposizioni ICT in corso di validità può essere consultata attraverso i canali di comunicazione di BMS oppure ritirata presso il reparto HR o il proprio superiore.

Assunzione di responsabilità

I collaboratori possono contribuire ad aumentare il livello di sicurezza indipendentemente dalla loro funzione e posizione gerarchica, prendendo coscienza della propria responsabilità personale.

Conoscenza di regolamenti e norme di sicurezza

I collaboratori devono familiarizzare con le presenti disposizioni e con le altre norme di sicurezza di BMS, rivolgendosi all'help desk IT o al proprio superiore per eventuali chiarimenti.
BMS si riserva il diritto di perseguire qualsiasi violazione delle presenti disposizioni in conformità con gli articoli 3.1 e 3.8 del regolamento del personale.

Segnalazione di punti deboli

Al verificarsi di incidenti critici o all'individuazione di punti deboli, BMS confida nel pronto intervento dei suoi collaboratori, che hanno il compito di informare l'help desk IT o il proprio superiore PER TELEFONO. Attenzione: non inoltrare tentativi di phishing, ransomware o altre minacce per e-mail all'help desk o ad altri utenti della rete BMS. Il messaggio a rischio deve essere immediatamente cancellato o contrassegnato come SPAM. Se un virus risulta già sottoposto a quarantena, non occorre attuare ulteriori misure, limitandosi a contattare l'help desk IT in caso di dubbi. I collaboratori non devono verificare di persona i punti deboli individuati o presunti.

Supporto ai colleghi di lavoro

I collaboratori possono aiutare i propri colleghi, segnalando loro i rischi per la sicurezza individuati. Un consiglio amichevole spesso è molto più utile di una normativa.

Uso di software e hardware

Hardware e software privati
L'utilizzo di apparecchi privati come PC/notebook o dispositivi di rete nelle aziende BMS è espressamente vietato. Non è inoltre consentito elaborare o memorizzare informazioni riservate di BMS su apparecchi personali presso la propria abitazione, fatta eccezione per

- Gli utenti in possesso di relativa autorizzazione scritta del reparto IT riguardante l'uso dei loro dispositivi privati.
- I collaboratori interni ed esterni o gli ospiti che utilizzano la rete Wi-Fi per i visitatori.
- La sincronizzazione della rubrica professionale di e-mail e calendario con smartphone e tablet privati è consentita **solo con l'account Exchange di BMS** e non con iCloud o qualsiasi altra directory privata (basata su cloud o meno). Gli utenti accettano esplicitamente la configurazione automatica dei dispositivi secondo le norme di sicurezza durante la sincronizzazione.

Acquisto, installazione e smaltimento di attrezzature e software
Il nuovo hardware e software e i nuovi servizi devono essere acquistati e installati tramite il reparto IT. A tal fine, i collaboratori devono utilizzare l'apposito modulo disponibile sul portale self-service Astra nell'Intranet BMS. Il modulo viene presentato al reparto IT (tramite l'help desk) per l'approvazione da parte del diretto superiore e del reparto HR prima dell'attivazione di un ticket di «richiesta» nel nostro sistema di ticketing (attualmente helpline).
Questa procedura si applica anche al freeware (software disponibile gratuitamente), ai prodotti open source (codice sorgente disponibile gratuitamente) o ai servizi cloud. Il software utilizzato deve essere concesso in licenza senza eccezioni. Inoltre, occorre assicurarsi che il software installato non sia copiato illegalmente. L'installazione di software privato è vietata.

I dispositivi dismessi vengono puliti superficialmente e restituiti al reparto IT, **completi di tutti gli accessori come caricabatterie, custodie, ecc**. Computer portatili e desktop vengono resettati completamente dal reparto di assistenza IT, che assicura così la cancellazione di tutti i dati. I documenti privati possono essere salvati su una chiavetta USB e cancellati dal laptop/desktop prima della consegna. **Gli iPhone dovrebbero essere completamente scollegati da qualsiasi account iCloud e riportati alle impostazioni di fabbrica** prima di essere restituiti al reparto di assistenza IT. I collaboratori che non eseguono questo passaggio prima della consegna possono essere chiamati a sostenere eventuali costi conseguenti.

Memoria cloud
Il salvataggio di dati tramite servizi cloud privati come Dropbox, OneDrive, Box, Drive e simili non è consentito. Eventuali casi di necessità devono essere notificati al reparto IT.

Guasti/furto di hardware e software
Tutti i guasti a software e dispositivi devono essere notificati senza indugio al superiore e all'help desk IT. Il furto di software e dispositivi deve per prima cosa essere denunciato tempestivamente alla polizia. La prova della denuncia (scansione o documento originale) deve essere presentata

all'help desk IT per mezzo di un ticket (il documento è necessario per la notifica all'assicurazione di responsabilità civile). I collaboratori possono essere ritenuti responsabili e sanzionati per danni all'hardware o al software provocati intenzionalmente o per negligenza grave, in conformità con gli articoli 3.1 e 3.8 del regolamento del personale.

Uso, cura e pulizia dei dispositivi

I dispositivi ICT di BMS devono essere utilizzati secondo le istruzioni del reparto IT. Il materiale non deve essere modificato in modo né permanente né superficiale (ad esempio con adesivi) senza il consenso del reparto IT. Ogni impiego anomalo di un dispositivo deve essere immediatamente notificato al reparto IT.
I collaboratori stessi sono responsabili della cura e della pulizia esterna dei dispositivi di BMS. L'hardware sottoposto a corretta manutenzione dura più a lungo ed è meno soggetto a guasti. A tal fine: tenere cibi e bevande a distanza di sicurezza da tastiere e dispositivi.

Uso di mezzi di comunicazione

Regolamento per l'uso di internet, e-mail, telefonia e comunicazioni su Beekeeper

- BMS fornisce l'accesso a internet per scopi aziendali a tutti i collaboratori autorizzati all'uso di dispositivi IT.

- I collaboratori sono personalmente responsabili delle proprie azioni. L'accesso a internet è limitato da un filtro web, che restringe il campo dei servizi disponibili in rete, bloccando i contenuti vietati o potenzialmente dannosi per BMS.

- Le restrizioni imposte dal filtro web sono vincolanti e non devono essere aggirate.

- Il download di materiale proibito dalla legge (in particolare rappresentazioni pornografiche, materiale politico estremo, ecc.) così come le violazioni del diritto d'autore sono vietati e possono comportare conseguenze penali per l'utente, nonché sanzioni come previsto dal regolamento del personale di BMS.

- L'uso occasionale di internet e del telefono aziendale (per chiamate) per scopi privati è consentito, purché ciò non pregiudichi la produttività dei collaboratori durante l'orario di lavoro.

- Qualora uno smartphone privato venga utilizzato anche come telefono aziendale, si applica quanto segue:
  - Non sono ammesse sincronizzazioni private su cloud.
  - La rubrica aziendale può essere sincronizzata SOLO con il server Exchange di BMS.
  - È vietato salvare qualsiasi registrazione digitale (video, foto, audio, ecc.) di dati BMS su supporti di memoria privati (interni o aggiuntivi).

- Utilizzando internet, gli utenti riconoscono espressamente il diritto di BMS di registrare il traffico di dati nel quadro dei fondamenti giuridici e di valutarlo nell'ambito della legge applicabile sulla protezione dei dati.

- **L'indirizzo e-mail aziendale non deve essere usato a scopi privati.** L'account di posta elettronica di un collaboratore che lasci l'azienda, così come tutti gli altri account IT e la casella di posta in arrivo, vengono salvati e bloccati al più tardi l'ultimo giorno lavorativo, per essere poi cancellati dopo un determinato periodo di tempo.
  Gli account di posta elettronica dei collaboratori in uscita dall'azienda o in congedo prolungato per malattia, che non abbiano avuto la possibilità di assegnare le proprie

operazioni in corso a un altro responsabile, possono essere esaminati alla ricerca di e-mail relative a dette operazioni, previa approvazione del reparto Legal & Compliance e secondo il principio del doppio controllo. Se la ricerca, contrariamente alle aspettative, dovesse evidenziare la presenza di e-mail private, le stesse saranno eliminate senza essere visionate.

- Il monitoraggio del traffico di posta elettronica aziendale si svolge nel quadro delle relative disposizioni legali. BMS adotta la seguente procedura:
    - Al sospetto fondato di un grave comportamento illegittimo all'interno dell'azienda, tuttavia non riconducibile a un individuo specifico, il reparto HR deve presentare una richiesta di monitoraggio generico in forma scritta al reparto IT, che può a sua volta avviare tale procedura in forma generale e sommaria. Questo tipo di monitoraggio non rivela alcuna identità, ma qualora rafforzi il sospetto, il reparto HR può richiedere indagini più mirate.
    - Qualora il sospetto di comportamento illegittimo ricada su un determinato collaboratore, il reparto IT, previa richiesta scritta del reparto HR, potrà esaminarne l'account utente alla ricerca delle relative prove.
    - Le e-mail e i documenti contrassegnati come «privati» o le e-mail e i documenti chiaramente di natura privata (ad esempio con un termine affettuoso nella riga dell'oggetto) non saranno aperti dal reparto IT.
    - I collaboratori interessati dall'ispezione mirata del proprio account ne saranno informati al più tardi dopo l'operazione.
    - Tutte le attività di ispezione del reparto IT vengono seguite dal reparto Legal & Compliance.

  Le conseguenze in ambito di diritto del lavoro possono spaziare da un richiamo al licenziamento senza preavviso, a seconda della gravità della cattiva condotta venuta alla luce.

- Le e-mail di origine sconosciuta o equivoca dovrebbero essere cancellate immediatamente. In nessun caso si dovrebbero aprire file allegati sconosciuti o non richiesti.

- In caso di incertezze, è opportuno contattare TELEFONICAMENTE l'help desk IT prima di aprire un allegato di dubbia natura, che non va mai inoltrato all'help desk IT.

- L'invio via e-mail di numeri di carte di credito, password, codici segreti è espressamente vietato.

- Comunicazioni su Beekeeper. Si applicano le seguenti regole di utilizzo:
    - Ci affidiamo al senso di responsabilità dei collaboratori, che in caso di dubbi devono rivolgersi ai propri superiori o al reparto del personale.
    - L'uso di BMSmobile è disciplinato dalle stesse regole riguardanti l'impiego di telefoni cellulari.
    - Tutti i contenuti pubblicati su BMSmobile sono destinati esclusivamente all'uso interno e non devono essere inoltrati a soggetti esterni.
    - I contributi con contenuti razzisti, sessisti o offensivi per singoli collaboratori o gruppi di collaboratori sono espressamente vietati. BMS si riserva il diritto di cancellare qualsiasi contributo/contenuto che violi la regola suddetta.
    - BMSmobile non deve essere utilizzato in presenza dei clienti.

Ulteriori informazioni sono disponibili alla pagina stessa di Beekeeper, all'indirizzo https://bms.beekeeper.io/fairplay

Le seguenti azioni sono esplicitamente vietate:

- violare le leggi applicabili o i buoni costumi;
- aggirare una misura di sicurezza del servizio informatico;
- violare i diritti di proprietà industriale, i diritti d'autore, i diritti della personalità, i diritti di proprietà o altri diritti di terzi;
- trasmettere contenuti infetti da malware (virus, trojan, worm, spyware, adware) o qualsiasi altro programma in grado di danneggiare i software;
- utilizzare pagine o eseguire applicazioni che potrebbero danneggiare o provocare un guasto al funzionamento dei siti web di BMS, in particolare tramite modifiche alla struttura logica o fisica dei server o della rete;
- distribuire o attivare e-mail di massa indesiderate, non richieste o moleste, nonché altre notizie, promozioni pubblicitarie, sondaggi esterni (basati su web o meno), pubblicità o qualsiasi altro tipo di invito;
- accedere ad applicazioni, sistemi, servizi, tool, dati, account, reti o contenuti e utilizzarli senza previa autorizzazione scritta o per scopi non preventivati;
- disattivare, interrompere, eludere, interferire o violare in qualsiasi altro modo la sicurezza dei siti web;
- attaccare, abusare, interferire, interrompere e sfruttare gli utenti, i sistemi o i servizi, inclusi ma non limitati al Denial of Service (DoS), al monitoraggio, al crawl, allo spam, all'utilizzo di bot o di script.
- I collaboratori si impegnano inoltre ad astenersi dalle seguenti azioni:
  - pubblicare, inviare, ricevere o salvare contenuti osceni o non appropriati;
  - esternare minacce e molestie, porre in essere persecuzioni, diffamazioni prive di fondamento o inganni nei confronti di persone fisiche o giuridiche;
  - promuovere, incentivare, supportare o commercializzare, in modo diretto o indiretto, prodotti commerciali, servizi, soluzioni o altre tecnologie di fornitori terzi;
  - attuare tentativi volti a raccogliere, salvare o pubblicare, attraverso i nostri siti web e/o i nostri profili, dati personali senza che la persona in questione ne sia a conoscenza e abbia fornito la sua autorizzazione;
  - inviare informazioni che identifichino fonti false o mendaci, inclusi «spoofing» e «phishing»;
  - partecipare ad attività illegali o criminali, come pedopornografia, gioco d'azzardo o pirateria, nonché incentivarle;
  - permettere, autorizzare o incoraggiare terze parti a porre in essere una delle azioni sopraccitate.

Gestione dei dati

Noi di BMS, in qualità di azienda e assieme ai nostri collaboratori, attribuiamo grande rilevanza all'accurata gestione dei dati che ci vengono affidati.

Non solo in virtù dell'obbligo previsto dalla legge sulla protezione dei dati e da altre disposizioni, ma soprattutto per l'importanza che attribuiamo alla tutela della personalità dei nostri collaboratori e clienti.

In tal senso, non fa alcuna differenza che i dati siano su carta o memorizzati in un computer.

In questo contesto, si devono osservare i seguenti punti:

Trattamento dei dati
Con l'account utente i collaboratori ottengono l'accesso a dati aziendali critici e riservati. Questi dati vengono visualizzati, trattati e archiviati esclusivamente per scopi commerciali, indipendentemente dal luogo di accesso (ufficio o accesso remoto).

La visualizzazione, il trattamento e l'archiviazione dei dati sono consentite solo con i dispositivi delle aziende BMS, fatta eccezione per la sincronizzazione di dati di e-mail e Intranet.

La responsabilità della corretta elaborazione dei dati aziendali è sempre a carico dei collaboratori.

Conservazione sicura delle informazioni
I documenti cartacei e gli altri supporti di dati contenenti informazioni riservate non devono rimanere esposti più del necessario e devono essere conservati sotto chiave dopo l'uso.

Si considerano riservati tutti quei documenti e quelle informazioni che descrivono circostanze interne o che potrebbero essere preziosi per la concorrenza. Anche le informazioni personali rientrano in questa categoria.

Sicurezza in sala riunioni
I collaboratori non devono lasciare documenti di lavoro confidenziali o qualsiasi informazione riservata su lavagne a fogli mobili e whiteboard nelle sale riunioni e tanto meno smaltire materiale sensibile nel cestino della carta straccia.

Smaltimento sicuro dei dati fisici
Il modo migliore per smaltire i documenti riservati è utilizzare un distruggidocumenti o, in mancanza di questa opzione, sminuzzarli fino a renderli illeggibili.

Salvataggio dei dati
I dati non devono essere memorizzati a livello locale sul computer, bensì nei sistemi centrali, dove BMS può assicurare la corretta applicazione degli elevati standard di protezione e sicurezza dei dati e, di conseguenza, la completa disponibilità dei prodotti del lavoro dei collaboratori anche dopo il reset o la sostituzione di un dispositivo. In caso contrario, in seguito a guasto, furto o uso errato del dispositivo, i dati vanno perduti.

Accesso remoto (accesso VPN)

- Ogni VPN di accesso remoto deve essere richiesta all'help desk IT da un superiore attraverso il sistema di ticketing.

- L'accesso remoto è consentito esclusivamente con un'autenticazione a 2 fattori. A tal fine l'assistenza IT mette a disposizione un'app per smartphone. Sui laptop/tablet di BMS è installato il client VPN «Global Protect».

- L'utente VPN necessita di: un account utente BMS, una versione attuale di Windows, una versione attuale di Citrix Workspace e una buona connessione Internet o una grande

larghezza di banda in presenza di più dispositivi a elevato consumo di banda (ad esempio, TV box, console di gioco, ecc.) collegati simultaneamente.

- Per l'accesso remoto, si applicano le stesse regole vigenti per la visualizzazione, il trattamento e l'archiviazione dei dati aziendali. È responsabilità dell'utente VPN assicurarsi che il proprio computer sia aggiornato e protetto (antivirus aggiornato, ecc.).

Sicurezza della postazione di lavoro

Sono molte le persone esterne che ogni giorno entrano ed escono dalle aziende di BMS: clienti, visitatori, operai, tecnici, addetti alle pulizie e alla vigilanza. Una postazione di lavoro ordinata è pertanto un fattore essenziale ai fini della sicurezza.

Applicazione della clean desk policy
In BMS vige la «clean desk policy». Questo significa che, in caso di interruzioni prolungate dell'attività, e al più tardi alla fine della giornata, tutti i documenti devono essere riordinati. I collaboratori che si assentino dalla propria postazione per un periodo di tempo più lungo, devono riporre le informazioni confidenziali su carta, i supporti dati, notebook e tablet in un luogo che possa essere chiuso a chiave.

Cautela con gli sconosciuti
Le porte devono essere sempre chiuse a chiave. Negli edifici senza reception si può aprire la porta agli estranei solo dopo essersi assicurati che siano autorizzati a entrare. I collaboratori devono segnalare persone o eventi sospetti ai loro superiori o al responsabile dell'edificio.

Il computer nell'area di vendita

Nelle filiali BMS i computer e i sistemi di cassa sono a volte situati nell'area di vendita, esponendo BMS al rischio di un accesso ai dispositivi da parte di clienti e visitatori. Per scongiurare questa eventualità:

- Attivare il blocco dell'accesso (Ctrl-Alt-Canc) quando ci si allontana dal luogo di lavoro, anche solo per un breve lasso di tempo.

- Prestare attenzione quando si inserisce la password (escludere la presenza di persone nelle vicinanze con visuale libera sullo schermo).

- Riservare l'uso dei dispositivi e dei servizi BMS alle persone che hanno accettato il regolamento del personale e le presenti disposizioni.

- Non permettere a visitatori e/o clienti di utilizzare il PC senza supervisione, nemmeno per brevi ricerche su internet.

Account utente personale

Ogni collaboratore ha un proprio account utente
L'account utente deve essere utilizzato esclusivamente dal titolare. I collaboratori devono utilizzare sempre e soltanto il proprio account utente. Sono ammesse eccezioni per gli account utente generici, ad esempio nei nostri negozi al banco di vendita, dove lo stesso account generico può essere utilizzato da un massimo di tre utenti.

Al sospetto che un account utente e la password associata siano o siano stati usati impropriamente da terzi, occorre darne immediata comunicazione al reparto IT tramite l'help desk IT.

Blocco del computer

Il computer deve essere bloccato anche in caso di brevi assenze (Ctrl + Alt + Canc). Prima di allontanarsi dalla postazione di lavoro (riunioni, pausa pranzo, ecc.), i collaboratori devono effettuare il logout.

Gestione corretta della password

- La password di un account utente deve essere nota solo al rispettivo collaboratore. La password non deve essere rivelata a nessuno (nemmeno a un superiore, a un tecnico dell'assistenza IT, all'help desk IT, a un collaboratore del reparto HR, ecc.).

- La password va cambiata a intervalli regolari, in ogni caso quando il sistema invia il relativo promemoria, scegliendo ogni volta una combinazione completamente nuova. La password non deve contenere riferimenti al collaboratore, al suo reparto o alla sua funzione e deve essere inserita senza essere osservati. Se questo non è possibile, è necessario modificarla al più presto.

- La password non deve mai essere memorizzata nel dispositivo BMS o annotata su un foglio visibile anche ad altri.

Scelta di una password sicura

Una password deve essere facile da ricordare, ma difficile da indovinare. Al riguardo, è opportuno ricordare quanto segue:

Cose da evitare

- La password non deve contenere riferimenti alla propria persona. Le password basate su cognome, nome, data di nascita dei figli, nome dell'animale domestico, lavoro, hobby, ecc. sono facili da indovinare.

- Allo stesso modo, è meglio non utilizzare nomi di personalità, animali, personaggi dei fumetti, marche di auto, località, regioni, ecc.

- È preferibile evitare termini che si ritrovano nei dizionari, indipendentemente dalla lingua,

- così come sequenze di lettere («ABCD») o combinazioni di tasti consecutivi sulla tastiera («asdfg»).

- Le password non devono essere numerate (password 1, password 2, password 3).

Cose da fare

- Una password deve contenere un minimo di 8 caratteri,

- lettere maiuscole e minuscole,

- almeno un carattere speciale come «!» o «#» e una cifra.

- Si sconsiglia di impiegare le lettere é à è ü ö ä ç, presenti solo in alcune lingue.

- Non deve contenere parole rivelatrici, come il proprio nome.

- Le ultime 5 password non devono essere riutilizzate.

- Ci si può servire di alcuni accorgimenti, come nell'esempio seguente:
  - Parola di partenza: postaprivata
  - Lettere maiuscole/minuscole: PostAPrivata
  - Inserimento di cifre: P0stAPr1vata
  - Aggiunta di un simbolo speciale: P0stAPr1v@ta?

Ottenimento fraudolento di dati / Social engineering

Spie industriali, hacker e altre persone spesso fingono di essere qualcun altro per ottenere l'accesso ai sistemi interni, chiedendo abilmente numeri di telefono diretti, nomi di collaboratori, password o informazioni simili. Questo approccio, chiamato social hacking, aggira tutte le misure tecniche di sicurezza e prende di mira l'anello più debole della catena di sicurezza: l'essere umano.

Diffidare sempre
I collaboratori devono verificare l'identità degli sconosciuti alla ricerca di informazioni su una persona o sull'azienda, invitandoli a presentare una relativa richiesta scritta. Se si ha l'impressione che la persona al telefono si stia facendo passare per un collaboratore del reparto IT, riagganciare e contattare immediatamente l'help desk IT al numero fornito su BMSmobile.

Riportare gli eventi sospetti
Gli eventi sospetti devono essere riportati senza indugio al superiore e all'help desk IT.

Notebook e altri dispositivi mobili

Contrastare i furti
Notebook, tablet o smartphone non devono mai essere lasciati incustoditi, prestando particolare attenzione nelle stazioni, in treno o in altri luoghi pubblici. I notebook devono essere sempre trasportati come bagaglio a mano. Eventuali furti devono essere denunciati immediatamente alla polizia nonché riportati al superiore, all'help desk IT e al reparto Legal.

Solo per uso aziendale
I dispositivi mobili sono uno strumento di lavoro per uso aziendale e non devono essere impiegati da altre persone, neppure da amici e familiari.

A casa e in viaggio
Queste disposizioni si applicano anche all'uso di dispositivi di lavoro mobili, indipendentemente dall'orario e dal luogo, a casa o in viaggio.

Entrata in vigore

Le presenti disposizioni entrano in vigore il 7 giugno 2021, sostituendo tutte le precedenti versioni delle disposizioni ICT ed altri precedenti documenti in ambito ICT.