Policy utente

Sistema informativo

♂

Data: Giugno 2018
Versione: 1.0
Classificazione: Ad uso interno

Revisioni		
Versione	**Data**	**Modifiche**
1.0	Giugno 2018	Prima stesura

1. Sommario

2. PREMESSA E AMBITO DI APPLICAZIONE

Il documento fornisce le linee guida per utilizzare correttamente le dotazioni informatiche ai fini della sicurezza, delle informazioni aziendali elaborate, del rispetto delle leggi vigenti in materia e dell'impiego efficiente ed efficace delle risorse impiegate.

Le indicazioni di seguito riportate sono altresì coerenti con finalità e metodi indicati Regolamento UE 2016/679 (GDPR).

Quanto definito nel presente documento trova applicazione in **S.A.Ba.R S.p.A**; tutte le strutture aziendali coinvolte sono tenute ad un onere d'informativa verso la Dirigenza Aziendale, secondo le modalità esposte nella presente Policy.

Regole e principi nell'utilizzo degli apparati informatici

I dipendenti e i collaboratori, sono responsabili dell'utilizzo corretto e consapevole delle dotazioni informatiche e sono tenuti a conoscere ed a seguire quanto previsto dal presente documento e dalle altre politiche aziendali per la sicurezza; i destinatari sono altresì tenuti al rispetto delle specifiche norme comportamentali di seguito espressamente previste.

La policy di seguito riportata si applica a tutti gli utenti interni ed esterni che hanno accesso al sistema informativo S.A.Ba.R. S.p.A.

Il Nuovo Art. 4 dello Statuto dei Lavoratori

Nel Settembre 2015, attraverso il D.Lgs 151/2015 (c.d. "Jobs Act") è stato riscritto l'art. 4 dello Statuto dei Lavoratori, modificando la **disciplina in materia di strumenti utilizzati dal lavoratore per rendere l'attività lavorativa** (PC, PC portatile, smartphone, tablet, chiavetta Internet, etc.) e di **strumenti di controllo degli accessi e delle presenze** (badge).

A seguito delle novità introdotte, si ricorda che tutti i dati e le informazioni raccolte tramite gli strumenti sopraelencati potranno essere utilizzati a tutti i fini connessi al rapporto di lavoro a condizione che al lavoratore sia data adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli nel pieno rispetto del GDPR 2016/679.

I dati raccolti nel rispetto di quanto prescritto dalla norma possono, quindi, essere utilizzati dal datore di lavoro a tutti i fini connessi al rapporto di lavoro, ivi compreso quello diretto al controllo sull'esatto adempimento della prestazione lavorativa così come quello disciplinare.

Provvedimenti

In caso di violazione della politica aziendale, **S.A.Ba.R. S.p.A** si serva di adottare, applicando il principio di proporzionalità, le sanzioni previste dal CCNL con le modalità stabilite dall'articolo 7 dello Statuto dei lavoratori.

Resta inteso che l'uso illegittimo delle informazioni e della rete Internet (come ad esempio la violazione del copyright, l'accesso abusivo ai sistemi informatici, la violazione della disciplina a protezione dei dati personali, etc.) può avere rilievi civili e penali di cui risponde direttamente il dipendente.

3. I DATI PERSONALI

Scopo

I dati sono tra i beni più preziosi che un'azienda possa avere e come tali devono essere adeguatamente trattati e protetti.
Il primo passo da compiere per attuare una buona protezione dei dati è **definirne una classificazione** in base a criteri legislativi o criticità aziendali. Lo scopo di questo documento è indicare una classificazione dei dati.

Ambito di applicazione

La politica si applica a tutti gli utenti interni ed esterni che hanno accesso al sistema informativo di **S.A.Ba.R. S.p.A.**
Vengono considerati tutti i dati del sistema informativo (documenti, immagini, testo, suoni, ecc) su qualunque supporto.

Classificazione

Il Regolamento (UE) 2016/679 definisce **dato personale** qualsiasi informazione riguardante una persona fisica identificata o identificabile**,** direttamente o indirettamente con particolare riferimento ad un identificativo come nome, numero identificativo, dati relativi all'ubicazione, un identificativo online o elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Vengono poi identificate due sottocategorie di dati, che per la tipologia di dati che comprendono, necessitano di tutele particolari:

- **categorie particolari di dati personali:** dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza a sindacati nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **dati personali relativi a condanne penali e reati**: dati giudiziari che riguardano persone fisiche e che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, etc.) o la qualità di imputato o di indagato.

IL TRATTAMENTO DEI DATI

La Policy che segue, riguarda tutti coloro che trattano dati personali attraverso banche dati di clienti, utenti, fornitori, dipendenti, etc.

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Il principio della normativa è quello di **tutelare l'integrità e la riservatezza dei dati in tutte le fasi del trattamento** (durante quindi la raccolta, registrazione, correzione, trasmissione, distruzione, etc.)

Sicurezza del Trattamento (art. 32 GDPR)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento e/o il Responsabile del Trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano, tra l'altro, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Rischio privacy:

- distruzione o perdita di dati;
- accessi non autorizzato;
- trattamento non consentito;
- trattamento non conforme alle finalità della raccolta.

Le **misure tecniche ed organizzative** devono concernere:

- quantità dei dati raccolti
- estensione del loro trattamento
- periodo di conservazione e la loro accessibilità.

Le misure devono garantire inoltre che, per impostazione predefinita, i dati personali non siano resi accessibili a un numero indefinito di persone fisiche (diffusione) senza l'intervento di un incaricato al trattamento.

Le misure di sicurezza devono essere idonee, adeguate, opportune; le **misure tecniche** devono concernere, a seconda dei casi:

- la pseudonimizzazione e la crittografia dei dati personali, la minimizzazione dei dati;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Le **misure organizzative devono garantire:**

- che qualunque persona che agisce sotto l'autorità del Titolare e del Responsabile, e che ha accesso ai dati personali, possa elaborare i dati solo secondo le istruzioni impartite, salvo obblighi giuridici (policy interne sulla corretta gestione dei dati);
- che tutti i soggetti incaricati devono essere adeguatamente formati e/o informati;
- che siano previste forme di audit interni finalizzati al monitoraggio e riesame per la valutazione della conformità del trattamento in relazione agli obblighi indicati nel Regolamento GDPR.

4. Credenziali di accesso

Scopo

La finalità di questa politica è fornire le linee guida per la **creazione e la gestione delle credenziali di accesso** a qualsiasi sistema, servizio, struttura, dispositivo di pertinenza **S.A.Ba.R. S.p.A** che supporta o richiede l'uso di autentificazione.

Ambito di applicazione

La politica **si applica a tutti gli utenti** a cui sono state assegnate credenziali di accesso o ne sono responsabili.
I codici identificativi e le relative abilitazioni sono rilasciati dal Titolare del Trattamento o dal Responsabile dei Sistemi Informativi, le password utilizzate per accedere ai sistemi informativi **sono di responsabilità personale del dipendente.**

Politica

Comportamenti non consentiti

- Annotare credenziali di accesso (username, password, PIN, ecc) su carta, post-it o altro materiale/supporto esponendole al rischio di essere carpite da altri.
- Lasciare incustodita la propria postazione di lavoro, badge, chiavi, o altri dispositivi che consentono l'accesso ad aree il cui accesso è riservato solo a personale autorizzato.
- Comunicare o fornire ad altre persone (incluso al proprio capo) le credenziali di accesso via email, telefono, o qualsiasi altra forma.
- Salvare/inviare credenziali di accesso in file/documenti non opportunamente criptati.
- Riutilizzare password già usate in precedenza.
- Consentire ad altre persone di servirsi delle proprie credenziali di accesso o utilizzare quelle di cui non si è l'assegnatario.

Comportamenti da tenere

- Le **password di default devono essere cambiate al primo utilizzo.**
- Digitare username e password avendo cura che nessuno stia osservando.
- **Scegliere password robuste** in grado di non essere facilmente indovinate, le password devono:
  - Essere composte da **almeno 8 caratteri**.
  - Contenere **caratteri appartenenti ad almeno tre delle quattro categorie** seguenti: caratteri maiuscoli dell'alfabeto inglese (A-Z), caratteri minuscoli dell'alfabeto inglese (a-z), cifre (0-9), caratteri non alfabetici (ad esempio !, #, %)
  - Non devono contenere nomi di familiari, animali domestici, date di nascita o altre informazioni personali.
  - Non devono essere parole di senso compiuto o da sequenze facilmente digitabili (ad esempio 12345678).
  - Non devono contenere il nome dell'azienda o altre sue derivazioni.

Cambio password

Le password devono essere cambiate **ogni 6 mesi in caso di accesso a dati personali, ogni 3 mesi in caso di accesso a particolari categorie di dati o dati personali relativi a condanne penali e reati. Il cambio password deve essere effettuato dal dipendente allo scadere dei termini previsti.**

Gestione password in caso di assenza

In situazioni di emergenza, in caso di **assenze non programmate** (ad esempio per malattia), il Titolare del Trattamento autorizza l'Amministratore di Sistema (ove nominato) ad accedere al contenuto dello strumento di lavoro, forzando il sistema di password inserito dall'utente.

Al primo accesso successivo, l'utente dovrà modificare la password.

Monitoraggio

Il Titolare del Trattamento potrà effettuare verifiche sul rispetto delle regole di applicazione della presente policy.

5. Postazione di lavoro e uso PC

Scopo

La finalità di questa politica è fornire le linee guida da seguire in relazione alla **postazione di lavoro**.

Ambito di applicazione

La **politica si applica a tutti gli utenti interni ed esterni** ai quali **S.A.Ba.R. S.p.A** ha dato a disposizione una postazione di lavoro e/o PC.

Politica

La postazione di lavoro è un bene dell'Azienda che viene preso in carico dal dipendente al momento della consegna.

Il **dipendente è tenuto ad utilizzare la postazione esclusivamente per lo svolgimento delle proprie mansioni** e ad adottare tutte le cautele a garanzia del suo corretto funzionamento, nonché a tutelare le informazioni aziendali/personali accessibili o elaborate tramite il suo utilizzo.

L'utente deve **rivolgersi al proprio responsabile** nel caso in cui abbia dei **dubbi sulla natura delle informazioni** e sulle relative modalità di trattamento ed archiviazione.

Comportamenti non consentiti

- Salvare il materiale pertinente alla propria attività lavorativa esclusivamente sul proprio computer ovvero su strumenti di condivisione / archiviazione esterna / servizi cloud (drop box, chiavette, etc.), senza provvedere ad archiviare lo stesso anche sui server aziendali
- Salvare su computer, server o dispositivi di memorizzazione aziendali materiale non correlato alla propria attività lavorativa (ad esempio file musicali, video, ecc).
- **Eseguire copie non autorizzate di dati o software**, utilizzare o installare software non autorizzato o in violazione delle norme sul copyright.
- Modificare la configurazione hardware/software delle apparecchiature a disposizione.
- Concedere l'utilizzo della propria postazione di lavoro ad altri senza aver ricevuto relativa autorizzazione.
- **Lasciare documenti contenenti informazioni sensibili custoditi in modo non opportuno** sulla propria scrivania o comunque in luoghi in cui persone che non dovrebbero entrare in possesso di tali informazioni potrebbero farlo.
- **La stessa cura va tenuta per quanto riguarda dispositivi rimovibili e stampe prodotte su stampanti condivise da più utenti.**
- Tenere cibo e bevande in prossimità delle apparecchiature elettroniche (computer, monitor, stampanti, ecc)
- Eseguire connessioni remote ad altri pc privati interni / esterni o posti all'esterno della rete informatica di **S.A.Ba.R. S.p.A** senza esplicita autorizzazione.

Comportamenti da tenere

- Eseguire il **log out o bloccare il computer** quando ci si allontana dalla postazione di lavoro.
- **Spegnere il computer** al termine dell'orario di lavoro.
- **Salvare** sempre tutti i dati pertinenti alla propria attività lavorativa **sui server aziendali** nelle cartelle oggetto di backup.
- Trattare solo dati necessari e sufficienti per le finalità lavorative.
- Verificare che, in caso di allontanamento dal posto di lavoro, i contenitori degli archivi e banche dati (scrivanie, cassetti, armadi, computer, etc.) non siano oggetto di trattamento improprio.

Monitoraggio

Il Titolare del Trattamento potrà effettuare verifiche sul rispetto delle regole di utilizzo della postazione di lavoro e dell'uso del PC aziendale per finalità di controllo della sicurezza degli strumenti di lavoro, e dei dati aziendali, in occasione di rilevazione di anomalie/abusi e di violazioni delle norme di pubblica sicurezza e aziendali.

Ai sensi dell'art. 4 dello Statuto dei Lavoratori, i dati raccolti nel rispetto nella normativa sulla privacy, possono essere utilizzati dal datore di lavoro a tutti i fini connessi al rapporto di lavoro, ivi compreso quello diretto al controllo sull'esatto adempimento della prestazione lavorativa così come quello disciplinare.

6. E-mail

Scopo

Indicare le linee guida da seguire per un corretto ed adeguato **utilizzo della posta elettronica S.A.Ba.R. S.p.A.**

Ambito di applicazione

La politica **si applica a tutto il personale interno o esterno** al quale **S.A.Ba.R. S.p.A** ha fornito un account email.

Politica

La posta elettronica è uno **strumento di lavoro aziendale** il cui utilizzo deve essere correlato alle attività produttive, coerente con gli obiettivi aziendali, rispettoso delle regole di buon senso e conforme alle leggi vigenti in materia. **La posta elettronica aziendale non può in alcun modo essere utilizzato per fini personali.**

Comportamenti non consentiti

- **Utilizzare l'account di posta elettronica S.A.Ba.R. S.p.A per uso personale e/o conservare email di carattere privato o personale.**
- Utilizzare la posta elettronica per la creazione o la distribuzione di messaggi offensivi (compresi commenti su razza, sesso, aspetto fisico, disabilità, età, orientamento sessuale), messaggi dal contenuto pornografico, messaggi che rivelano l'orientamento politico o il credo religioso.
  Se si riceve un'email con contenuti offensivi inviata da una qualsiasi persona riferibile a **S.A.Ba.R. S.p.A** è necessario segnalare l'accaduto al proprio responsabile.
- **Inviare mail contenenti particolari categorie di dati** (sensibili, biometrici, convinzioni politiche, religiose, etc.) **o dati personali relativi a condanne penali e reati senza esplicita autorizzazione** da parte del proprio Responsabile. In ogni caso l'informazione deve esser adeguatamente criptata/protetta.
- Pubblicare, salvo autorizzazione, l'account di posta elettronica **S.A.Ba.R. S.p.A** su Internet o utilizzarlo per registrarsi a siti non strettamente legati all'attività aziendale (ad esempio forum, blog, social network, ecc).
- Inviare messaggi di posta utilizzando account **S.A.Ba.R. S.p.A** assegnati ad altre persone.
- Lasciare incustodite eventuali stampe di messaggi di posta elettronica contenenti informazioni sensibili, giudiziari e/o riservati.
- Impostare l'inoltro automatico della posta ricevuta verso un altro destinatario, ad eccezione dei casi descritti in seguito relativi alla gestione delle mail durante i periodi di assenza.
- Inviare in chiaro (cioè non adeguatamente criptate) via email credenziali di accesso (username, password, PIN, ecc).
- Configurare sul computer aziendale account di posta personali;
- Disinstallare o comunque impedire l'utilizzo di sistemi di filtraggio delle mail che sono utilizzati a protezione degli apparati informatici e delle informazioni in essi conservate;
- Utilizzare account di posta elettronica non aziendali per lo svolgimento di mansioni lavorative;
- Cancellare e-mail di pertinenza aziendale.

Comportamenti da tenere

- Inserire sempre un Oggetto nel relativo campo del messaggio che si sta inviando.
- **Segnalare all'Amministratore di Sistema eventuali avvisi riguardanti virus, phishing o altre anomalie.**
- Controllare la posta frequentemente.
- Verificare che i destinatari inseriti siano quelli corretti prima di inviare un messaggio di posta.
- Evitare di inviare messaggi con allegati di grosse dimensioni.
- Non stampare i messaggi di posta elettronica se non strettamente necessario.
- Nel caso in cui un **messaggio di posta elettronica** debba essere **inviato ad una lista di destinatari utilizzare il campo Ccn** per l'inserimento degli indirizzi di destinazione. Il campo cc deve essere utilizzato solo nel caso in cui sia opportuno/necessario che i destinatari del messaggio vengano a conoscenza degli indirizzi degli altri destinatari.

Gestione email in caso di assenza

In caso di **assenze programmate** (ad esempio per ferie o attività di lavoro fuori sede) occorre:

- **attivare l'invio di una risposta automatica** contenente le "coordinate" (telefoniche o elettroniche) di un altro soggetto o altre modalità di contatto della struttura;
- **attivare l'inoltro delle mail all'indirizzo condiviso dall'ufficio** (ove presente) o altro indirizzo mail (collega o responsabile).

In caso di **assenze non programmate** (ad esempio per malattia) e/o qualora il lavoratore non possa attivare la procedura sopradescritta, il Titolare del Trattamento autorizza l'Amministratore di Sistema (ove nominato) ad accedere al contenuto della casella di posta e/o impostare l'invio di una risposta automatica e l'inoltro delle e-mail ad altro contatto aziendale. Al primo accesso successivo, l'utente dovrà modificare la password.

Gestione email in caso di dimissioni/licenziamento/esclusione

In caso di **dimissioni/licenziamento/esclusione del lavoratore intestatario della casella di posta elettronica**, il Titolare del Trattamento autorizza l'Amministratore di Sistema (ove nominato) ad impostare l'invio di una risposta automatica ed inoltrare le e-mail ad altro contatto aziendale.
La casella di posta elettronica verrà poi definitivamente chiusa entro 12 mesi dalle dimissioni.

Gestione email in caso di dimissioni/licenziamento/esclusione

In caso di **dimissioni/licenziamento/esclusione del lavoratore intestatario della casella di posta elettronica**, l'Amministratore di Sistema sarà autorizzato ad impostare l'invio di una risposta automatica ed inoltrare le e-mail ad altro contatto aziendale.
La casella di posta elettronica verrà poi definitivamente chiusa entro 12 mesi dalle dimissioni.

Filtri

A protezione degli apparati informatici e delle informazioni in essi conservate, **S.A.Ba.R. S.p.A** ha adottato un **sistema di filtraggio delle mail ricevute.**

Monitoraggio e controlli

Il Titolare del Trattamento può effettuare **monitoraggi sul sistema di posta elettronica** allo scopo di verificare la sua efficienza e funzionalità.

Nel caso in cui i preventivi accorgimenti tecnici non abbiano impedito un evento dannoso o una situazione di pericolo, possono essere adottate misure volte a verificare se tali eventi o situazioni siano determinati da

eventuali comportamenti anomali.

In questo caso, se possibile, viene effettuato un *controllo preliminare su dati aggregati*, riferiti all'intera struttura lavorativa o a sue aree o ancora, se necessario, su base individuale. Il controllo può concludersi con un avviso generalizzato o individuale relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

Ai sensi dell'art. 4 dello Statuto dei Lavoratori, i dati raccolti nel rispetto nella normativa sulla privacy, possono essere utilizzati dal datore di lavoro a tutti i fini connessi al rapporto di lavoro, ivi compreso quello diretto al controllo sull'esatto adempimento della prestazione lavorativa così come quello disciplinare.

7. Internet

Scopo

La finalità di questa policy è indicare le linee guida da seguire per un corretto ed adeguato utilizzo di Internet.

Ambito di applicazione

La politica si applica a **tutti gli utenti interni ed esterni** a cui **S.A.Ba.R. S.p.A** ha concesso l'uso di Internet.

Politica

È possibile accedere a Internet solo dopo essere stati autorizzati da **S.A.Ba.R. S.p.A.** L'autorizzazione all'accesso può essere revocata in ogni momento, così come è sempre possibile limitare l'uso di Internet a determinati servizi e funzionalità.

L'utilizzo di Internet deve essere correlato alle attività produttive, coerente con gli obiettivi aziendali, rispettoso delle regole di buon senso e conforme alle leggi vigenti in materia. **La navigazione Internet a fini personali non è consentita.**

Comportamenti non consentiti

- Usufruire del servizio Internet per **scopi vietati dalla legislazione vigente.**
- **Scaricare o diffondere:**
  - materiale protetto da **copyright o software/informazioni per eludere diritti d'autore** (crack, licenze d'uso, ecc).
  - materiale **pornografico, pedopornografico, di carattere offensivo** (compresi commenti su razza, sesso, aspetto fisico, disabilità, età, religione, orientamento sessuale e politico, e contenuti incitanti all'odio e all'illegalità).
  - **file, programmi o contenuti non legati alla propria attività lavorativa** (ad esempio file audio, video, immagini).
- **Navigare su siti web:**
  - **pedopornografici, pornografici**.
  - di **carattere offensivo** (compresi commenti su razza, sesso, aspetto fisico, disabilità, età, religione, orientamento sessuale e politico, e contenuti incitanti all'odio e all'illegalità).
  - **direttamente o indirettamente finalizzati ad eludere diritti d'autore** (crack, licenze d'uso, ecc).
  - **file, programmi o contenuti non legati alla propria attività lavorativa.**
- **Accedere ad Internet in orari differenti da quello di lavoro**.
- Collegarsi ad Internet da postazioni aziendali attraverso chiavette o, altri dispositivi, senza esplicita autorizzazione.
- **Utilizzare Internet per finalità non pertinenti al proprio lavoro** (finalità personali, ludiche, economiche quali acquisti di beni e servizi, abbonamenti, pagamenti, ecc).
- Accedere alla rete **S.A.Ba.R. S.p.A** dall'esterno con qualsiasi mezzo di accesso remoto salvo esplicita autorizzazione ovvero accedere a computer/sistemi esterni alla rete **S.A.Ba.R. S.p.A** senza autorizzazione.
- Svolgere qualsiasi attività per tentare di eludere i sistemi di controllo di accesso e/o sicurezza di qualsiasi apparecchiatura interna o esterna, incluso il possesso o l'uso di strumenti software per tentare di rivelare password, identificare eventuali vulnerabilità di sicurezza, decriptare file crittografati, compromettere la sicurezza del sistema informativo.
- Installare o eseguire senza autorizzazione sui dispositivi aziendali software scaricato da Internet.

- Divulgare/diffondere su Internet contenuti che sono, o potrebbero essere, in contrasto con le politiche della società, informazioni sensibili, informazioni aziendali di qualsiasi natura (indirizzi di posta, ecc) senza aver ricevuto esplicita autorizzazione.

Filtri

S.A.Ba.R S.p.A applica dei filtri preventivi per ridurre il rischio di usi impropri della navigazione Internet consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti (ad esempio social network, peer-to-peer, chat, ecc), l'upload o il download di file, l'uso di servizi o applicazioni con finalità ludiche o estranee all'attività lavorativa.

Monitoraggio e controlli

Il Titolare del Trattamento potrà effettuare verifiche sul rispetto delle regole di utilizzo della connessione Internet per finalità di controllo della sicurezza e funzionalità della connessione, e dei dati aziendali, in occasione di rilevazione di anomalie/abusi e di violazioni delle norme di pubblica sicurezza e aziendali.
In questo caso, se possibile, viene effettuato un *controllo preliminare su dati aggregati*, riferiti all'intera struttura lavorativa o a sue aree o ancora, se necessario, su base individuale. Il controllo può concludersi con un avviso generalizzato o individuale relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

Ai sensi dell'art. 4 dello Statuto dei Lavoratori, i dati raccolti nel rispetto nella normativa sulla privacy, possono essere utilizzati dal datore di lavoro a tutti i fini connessi al rapporto di lavoro, ivi compreso quello diretto al controllo sull'esatto adempimento della prestazione lavorativa così come quello disciplinare.

8. Antivirus

Scopo

La finalità di questa policy è indicare le linee guida da seguire per **ridurre il rischio di infezioni da virus informatici**.

Ambito di applicazione

La politica si applica a **tutti gli utenti interni ed esterni.**

Politica

Sui computer aziendali **deve essere utilizzato solo software antivirus autorizzato** da **S.A.Ba.R. S.p.A**. Ogni giorno vengono scoperti nuovi virus. **L'antivirus aziendale viene mantenuto costantemente aggiornato.**

Comportamenti non consentiti

- Aprire file allegati ad un messaggio email proveniente da un mittente sconosciuto o sospetto.
- Scaricare, aprire o eseguire file di cui si ignora la funzione o provenienti da fonti sconosciute, non sicure, sospette.
- Eseguire macro contenute in documenti (ad esempio documenti Word o Excel) se non ne si conosce la finalità.
- Permettere che eventuali dimostrazioni commerciali, o di qualsiasi natura, realizzate da personale esterno (fornitori, ecc) vengano eseguite su postazioni **S.A.Ba.R. S.p.A**.

Comportamenti da tenere

- Cancellare messaggi email di spam o dal contenuto/mittente sospetto o sconosciuto senza inoltrarli ad altri destinatari.
- Salvare i dati aziendali sulle cartelle dei server **S.A.Ba.R. S.p.A** oggetto di backup. In questo modo sarà possibile recuperare, integralmente o in parte, le informazioni andate eventualmente perse a causa di virus.
- Eseguire sempre una scansione con il software antivirus dei dispositivi rimovibili (ad esempio chiavette USB, CD/DVD, ecc) prima di procedere al loro utilizzo sui computer aziendali.
- Segnalare eventuali malfunzionamenti del software antivirus o avvisi di virus rilevati sulla postazione in uso.
- Nel dubbio eseguire sempre una scansione con il software antivirus.

Monitoraggio

L'antivirus aziendale viene monitorato centralmente. Si ha in tempo reale la panoramica su tutte le postazioni in cui è installato.

9. Dispositivi rimovibili

Scopo

La finalità di questa policy è indicare le linee guida da seguire nell'utilizzo di dispositivi rimovibili (ad esempio chiavette USB, hard disk portatili, ecc) per ridurre l'esposizione al rischio di infezioni da malware/virus e perdita o divulgazione di informazioni sensibili.

Ambito di applicazione

La policy si applica al **personale** interno o esterno che utilizza dispositivi di archiviazione removibili per accedere al sistema informativo aziendale.

Politica

Comportamenti non consentiti

- Salvare su dispositivi rimovibili informazioni aziendali a meno che non sia strettamente necessario per la propria attività lavorativa e senza che lo stesso sia già stato archiviato anche sui server aziendali. In ogni caso l'informazione deve esser adeguatamente criptata/protetta.
- Utilizzare, salvo autorizzazione, i dispositivi rimovibili forniti da **S.A.Ba.R. S.p.A**, su apparecchiature non aziendali o per finalità non legate alla propria attività lavorativa.
- Impiegare dispositivi rimovibili personali su apparecchiature aziendali.

Comportamenti da tenere

- Eseguire sempre una scansione antivirus prima di utilizzare un dispositivo rimovibile.
- Conservare con cura i dispositivi rimovibili forniti dall'azienda.

10. Accesso remoto

Scopo

La finalità di questa policy è indicare le linee guida da seguire in relazione alle **connessioni remote**.

Ambito di applicazione

La policy si applica al **personale interno ed esterno** che è stato autorizzato ad eseguire accessi da remoto.

Politica

Per accedere da remoto alla rete **S.A.Ba.R. S.p.A** occorre essere stati autorizzati. L'autorizzazione viene assegnata individualmente e verrà fornita indicazione sulle modalità di connessione da utilizzare.

Comportamenti non consentiti

- Accedere da remoto alla rete **S.A.Ba.R. S.p.A** senza essere stati autorizzati a farlo o con modalità diverse da quelle indicate/permesse.
- Utilizzare credenziali di cui non si è l'assegnatario o permettere ad altri di usufruire delle proprie.
- Eseguire connessioni remote alla rete interna **S.A.Ba.R. S.p.A** da computer non aziendali salvo esplicita autorizzazione.
- Accedere remotamente dalla rete aziendale, salvo autorizzazione, a computer/dispositivi posti all'esterno di essa.

Comportamenti da tenere

- È responsabilità dell'utente che esegue il collegamento remoto assicurarsi che non vengano realizzati accessi non autorizzati (ad esempio da parte di membri della propria famiglia) e potenzialmente dannosi a risorse o informazioni aziendali.
- Eseguendo una connessione da remoto alla rete interna è come se ci si trovasse in ufficio. Valgono pertanto tutte le policy riferibili al sistema informativo **S.A.Ba.R. S.p.A**.

Monitoraggio

Gli accessi remoti saranno oggetto di log.

11. Come verificare se la connessione ad un sito web è sicura

Il pulsante di identificazione del sito (un lucchetto) compare nella Barra degli indirizzi quando si visita un sito web sicuro. In questo modo si potrà sapere velocemente se la connessione con il sito web visitato è protetta da cifratura e, in alcuni casi, a chi è intestato quel sito web. Queste informazioni aiuteranno a evitare quei siti web malevoli progettati allo scopo di sottrarre dati sensibili.

Il pulsante di identificazione del sito è posizionato alla sinistra dell'indirizzo web. Durante la visualizzazione di una pagina web, il pulsante visualizzerà solitamente l'icona di un lucchetto verde.

In alcune occasioni può invece visualizzare l'icona di un lucchetto grigio con un segnale triangolare giallo di avvertimento o un lucchetto spezzato (un lucchetto attraversato da una barra diagonale rossa).

Nota: facendo clic sul pulsante si aprirà il Centro controllo che consente di accedere a informazioni più dettagliate relative alla sicurezza della connessione al sito web. Permette inoltre di modificare alcune impostazioni relative a privacy e sicurezza.

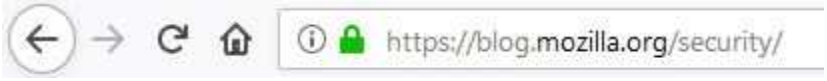
Indice dei contenuti

ATTENZIONE: non inviare mai dati sensibili (ad esempio coordinate bancarie, numeri di carta di credito e simili) a siti web quando nella Barra degli indirizzi non compare l'icona del lucchetto. In questi casi non vi è la certezza che la connessione sia effettivamente instaurata con il sito web indicato, né che tale connessione sia protetta da eventuali tentativi di intercettazione.

12. Lucchetto verde

Il lucchetto verde (con o senza il nome dell'organizzazione) indica che:

- La connessione è avvenuta certamente con il sito il cui indirizzo compare nella Barra degli indirizzi e non è stata intercettata.
- La connessione instaurata con Firefox verso quel sito è cifrata e considerata quindi sicura dai tentativi di intercettazione.



Quando accanto al lucchetto verde compare anche il nome dell'organizzazione (in verde), vuol dire che il sito sta utilizzando un certificato di validazione estesa (EV). Per ottenere un certificato EV, un tipo speciale di certificato, è richiesto un processo di verifica dell'identità significativamente più rigoroso rispetto agli altri tipi di certificato.

Per i siti web che utilizzano certificati EV, il pulsante di identificazione del sito mostra un lucchetto verde con accanto il nome giuridico della società o dell'organizzazione e l'ubicazione del soggetto che possiede il sito web (ad esempio, indicherà che la Fondazione Mozilla possiede mozilla.org).

13. Lucchetto grigio con triangolo giallo di avvertimento

Un lucchetto grigio con segnale triangolare giallo di avvertimento indica che la connessione tra Firefox e il sito web è solo parzialmente cifrata e non è protetta da eventuali tentativi di intercettazione. Compare anche quando si visitano siti web i cui certificati sono autofirmati o non sono rilasciati da un'autorità di certificazione attendibile.

Per informazioni sul significato dell'espressione "parzialmente cifrata", leggere l'articolo Blocco dei contenuti non sicuri delle pagine web. La risoluzione di questo problema spetta agli sviluppatori del sito web.

Nota: non inviare mai dati sensibili come coordinate bancarie, numeri di carta di credito e simili a siti web dove compare l'icona con il triangolo giallo di avvertimento.

14. Lucchetto grigio con barra rossa

Un lucchetto attraversato da una barra rossa indica che la connessione tra Firefox è solo parzialmente cifrata e pertanto non è da considerarsi sicura contro possibili tentativi di intercettazione o attacchi di tipo *man in the middle*.

Questa icona non comparirà se non nel caso in cui si sia disattivato il blocco dei contenuti misti.

Nota: non inviare mai dati sensibili come coordinate bancarie, numeri di carta di credito e simili a siti web dove compare l'icona del lucchetto grigio barrato di rosso.