Istruzione privacy **Policy per l'utilizzo delle risorse informatiche**	*Codice* **IP02**

*Il sottoscritto assicura che il presente documento è copia conforme dell'originale disponibile nella bacheca elettronica della **BTP SPA** alla data di consegna. L'eventuale revisione aggiornata è disponibile nell'area riservata di www.btpspa.it.*	*Distribuito a scopo informativo e non soggetto ad aggiornamento:*
Data consegna: / *Destinatario:*	*Distribuito in copia controllata:*

Rev.	Data	Descrizione modifiche	Redatto	Verificato	Approvato
01.a	*1/01/06*	*Prima stesura*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
01.b	*01/01/07*	*Modifiche formali*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
02.a	*01/01/09*	*Aggiornamento*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*

1. Oggetto

La presente Policy viene redatta dalla società BTP SPA (d'ora in avanti: azienda), al fine di regolamentare l'utilizzo delle proprie risorse informatiche da parte del personale dipendente e non dipendente comunque ad essa legato da un contratto di lavoro subordinato, di prestazione d'opera occasionale, di rapporti di collaborazione a progetto, di lavoro interinale, collaborazioni occasionali (d'ora in avanti: il contratto di lavoro; i lavoratori).

La presente Policy si rivolge sia a coloro che prestano il proprio lavoro o la propria opera nelle sedi dell'azienda compresi i cantieri mobili, sia a coloro che svolgono la propria prestazione con contratto di lavoro subordinato in luogo diverso dalla sede di lavoro per il mezzo della tecnologia informatica (telelavoro nelle forme dell'ufficio satellite, del telelavoro mobile, del telelavoro a domicilio, ...).

Una copia della presente Policy viene inviata per posta elettronica ad ogni lavoratore che, con la lettura ne accetta il contenuto o segnala qualunque dubbio o perplessità al Responsabile della Sicurezza Informatica. Il presente documento integra il contratto individuale per le materie che disciplina. L'inosservanza delle regole di comportamento contenute nella presente Policy configura per i dipendenti altrettanti illeciti disciplinari la cui previsione integra il codice disciplinare vigente. Una copia della presente Policy è disponibile sul sito aziendale www.btpspa.it .

2. Premessa

La legislazione italiana prevede sanzioni per le imprese che non vigilino sull'osservanza di modelli organizzativi volti a prevenire la commissione di specifici reati da parte degli stessi vertici aziendali (d.lg. n. 231/2001) ed impone all'azienda di controllare il corretto impiego degli strumenti aziendali per la produzione e di dettare le disposizioni per il corretto utilizzo degli stessi, di cui essa assume le responsabilità nei confronti del personale dipendente e non dipendente nonché nei confronti dei terzi. In particolare l'entrata in vigore del D.Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) introduce rilevanti obblighi a carico dell'azienda sanzionati civilmente e penalmente imponendo di trattare i dati personali rispettando il diritto di riservatezza degli interessati, prescrivendo un trattamento lecito e corretto.

La presente Policy si pone l'obiettivo di creare una "buona pratica" nelle relazioni di lavoro improntate alla trasparenza, all'accordo e all'uniformità dei comportamenti.

Essa intende, pertanto, garantire il datore di lavoro, il quale ha diritto di richiedere una corretta esecuzione della prestazione lavorativa; ma anche i lavoratori che vengono, in tal modo, resi edotti della politica aziendale in materia di utilizzo di risorse informatiche.

3. Rispetto dello Statuto dei lavoratori e della disciplina della privacy

La presente Policy intende regolamentare l'esercizio del potere di controllo, direttivo e disciplinare dell'azienda nei confronti dei lavoratori al solo ed esclusivo scopo di tutela del patrimonio aziendale.

L'azienda garantisce, pertanto, che non intende adottare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori; effettuare indagini ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore; violare la disciplina sulla tutela dei dati personali; violare la normativa sulla tutela della corrispondenza privata.

4. Utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet

L'azienda vuole tutelare i lavoratori interessati perché l'utilizzo della posta elettronica e della rete internet, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa.

L'utilizzo di Internet da parte dei lavoratori, se non limitato ai soli fini aziendali, potrebbe formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni.

Ancora maggiore è il rischio per i servizi di posta elettronica, se contengono dati personali ed eventualmente sensibili relativi ai lavoratori stessi o terzi identificati o identificabili, dato che sono suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza del contenuto della corrispondenza.

Per evitare di violare la privacy dei lavoratori è quindi necessario che essi si limitino ad un uso strettamente aziendale degli accessi ad internet e della posta elettronica.

5. Strumenti messi a disposizione dei lavoratori incaricati del trattamento dei dati con strumenti elettronici

Ad ogni lavoratore dell'azienda viene fornito un username (in genere formato dall'iniziale del nome seguita dal cognome) per l'accesso alla rete aziendale che è abilitato anche alla navigazione su internet.

Viene inoltre fornita una casella di posta aziendale alla quale, per semplicità, viene assegnato come indirizzo l'USERNAME (es. g.marullo@btpspa.it).

L'uso dell'iniziale del nome seguita dal cognome come indirizzo di posta è solo una semplificazione rispetto all'uso di un indirizzo esplicitamente riferito alla funzioni aziendali ricoperte dal lavoratore (es. g.marullo@btpspa è più semplice da comunicare rispetto a resp.sist.informatico.e.qualita@btpspa.it).

Se il lavoratore desidera è suo diritto chiedere ai Sistemi Informativi di non utilizzare lo standard aziendale ed **avere per la casella di posta un indirizzo che non sia riferibile al proprio nome e cognome** che sarà comunque utilizzabile solo dall'username assegnato.

La password associata all'usermane dovrà essere nota al solo lavoratore poiché garantirà l'associazione solo ad esso delle attività svolte con quell'username che potranno essere registrate in vari archivi e **contestate al lavoratore in caso di violazione di norme aziendali (es. comunicazioni all'esterno di informazioni riservate) o segnalate all'Autorità Giudiziaria in caso di responsabilità penali (es. navigazione su siti pedo-pornografici)**.

6. Responsabilità nell'utilizzo delle risorse informatiche

I lavoratori sono tenuti ad un uso corretto delle risorse e attrezzature messe a loro disposizione per l'esecuzione dell'attività lavorativa. Essi rispondono dei danni eventualmente occorsi sia durante l'esecuzione della prestazione lavorativa sia al di fuori della medesima, fintanto che risorse e attrezzature rientrino nella loro disponibilità.

L'utilizzo delle apparecchiature informatiche dovrà avvenire in conformità alle prescrizioni previste dall'Istruzione Operativa "Prescrizioni per gli incaricati del trattamento dei dati" disponibile, sempre nell'ultima versione aggiornata, nel sito www.btpspa.it.

In particolare si ricorda la finalità esclusivamente aziendale dell'uso dei portatili e il divieto di utilizzo degli stessi da parte di persone esterne all'azienda.

7. Proprietà e controllo del corretto utilizzo delle strutture aziendali

Compete ai datori di lavoro assicurare la funzionalità e il corretto impiego delle strutture aziendali da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali. E' inoltre necessario adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità.

L'azienda è pertanto tenuta a controllare il corretto impiego degli strumenti aziendali per la produzione ed a dettare le disposizioni per il corretto utilizzo degli stessi, di cui l'azienda assume la piena responsabilità nei confronti dei lavoratori e dei terzi.

L'azienda ha ritenuto di non individuare preventivamente tutte le categorie di siti considerati correlati o non correlati con la prestazione lavorativa (anche in relazione alla scarsa affidabilità di queste catalogazioni per i siti nazionali) e quindi ha solo parzialmente configurato i sistemi utilizzando filtri che prevengano determinate operazioni. E' lasciata quindi ad ogni lavoratore la responsabilità di un corretto utilizzo delle risorse messe a disposizione.

Per individuare eventuali attacchi ai quali è sottoposto il sistema è necessario effettuare periodicamente controlli che hanno lo scopo di individuare situazioni anomale. Nel tentativo di rispondere prontamente ad attacchi o situazioni particolari non prevedibili l'unica soluzione è un controllo analitico.

Gli strumenti software leader a livello mondiale nel settore della sicurezza informatica permettono all'amministratore del sistema di:

- registrare ed analizzare tutti i siti raggiunti navigando su internet (utente, ora, byte scaricati, indirizzo);
- analizzare il contenuto dei messaggi di posta sia inviati che ricevuti;
- analizzare il contenuto delle cartelle personali o di gruppo memorizzate sul server;
- analizzare il contenuto dei dischi del PC.

Le informazioni legate ai suddetti controlli sono memorizzate e salvate nelle copie di backup e quindi recuperabili anche a distanza di tempo. L'azienda tratterà comunque questi dati mediante opportune aggregazioni o in forma anonima o tale da precludere l'immediata identificazione degli utenti.

Per limitare l'arrivo di messaggi di posta indesiderata (SPAM) l'Azienda ha attivato un sistema Antispam che prevede il controllo degli indirizzi dei mittenti e del contenuto dei messaggi in ingresso. Questa attività è svolta da società esterne (con sedi all'estero).

In caso di guasti o malfunzionamenti delle apparecchiature elettroniche i responsabili delle società (esterne) addette alla manutenzione possono accedere a tutte le informazioni contenute nei dischi dei PC, su tutte le cartelle personali e di gruppo memorizzate sul server, al contenuto della posta.

Questi controlli, qualora gli utenti non si limitino ad un uso strettamente aziendale degli strumenti informatici, potrebbero rilevare dati "sensibili" (idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale) protetti dal D.Lgs. 196/2003 rendendo impossibile eseguire i controlli stessi. **Per consentire di compiere senza problemi questi controlli e queste attività è proibito un uso personale degli strumenti informatici, dell'accesso ad internet e della posta elettronica messi a disposizione dall'azienda.**

L'amministratore del sistema potrà quindi effettuare tutti i controlli (con la modalità concordate con le rappresentanze sindacali il 22/06/04)

senza per questo violare il D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali) ed in conformità con la delibera del Garante della privacy del 1 Marzo 2007 relativa alle linee guida per posta elettronica e internet.

8. Utilizzo delle risorse informatiche aziendali

Tutto quanto compone la dotazione delle risorse informatiche, l'accesso ad internet e la casella di posta elettronica con dominio aziendale (btpspa.it) appartengono al patrimonio aziendale.

I lavoratori utilizzano le risorse informatiche e quanto sopra solo ed esclusivamente per fini professionali per il perseguimento degli obiettivi fissati dall'azienda e quant'altro sia dalla stessa espressamente autorizzato.

La prescrizione riguarda l'intera attrezzatura messa a disposizione del lavoratore per lo svolgimento dell'attività lavorativa, ivi compresi il telefono cellulare ed il personal computer portatile e quant'altro possa servire.

L**'uso dell'iniziale del nome seguita dal cognome come username per l'accesso alle risorse informatiche aziendali non autorizza ad un uso privato delle stesse ma all'uso per le funzioni aziendali ricoperte dal lavoratore**. Ai lavoratori è quindi fatto espresso divieto di utilizzo delle risorse informatiche per scopi personali.

Ogni restrizione nell'utilizzo delle risorse informatiche aziendali è finalizzato a garantire idonee e preventive misure minime di sicurezza così come prescritte dal **D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali)** e successive modificazioni ed integrazioni.

N.B. E' possibile, ad esempio in caso di malfunzionamenti o di assenza imprevista del lavoratore, che una risorsa debba essere resa disponibile ad altri lavoratori o a società esterne. **E' quindi indispensabile che nessun dato personale sia presente sulle risorse informatiche aziendali neppure provvisoriamente.**

Ai lavoratori è fatto, altresì, espresso divieto di: modificare le configurazioni impostate sul proprio computer; ascoltare programmi e file audio e musicali; utilizzare programmi non distribuiti ufficialmente; scaricare file contenuti in supporti magnetici od ottici che non abbiano diretta attinenza con la prestazione lavorativa; navigare in siti non strettamente attinenti allo svolgimento della prestazione lavorativa, con particolare riferimento a quelli che possano rivelare le preferenze ed opinioni politiche, religiose, sessuali, o sindacali del dipendente. E' altresì vietata ogni forma di transazione finanziaria, commerciale.

9. L'utilizzo della casella di posta elettronica con dominio aziendale

I lavoratori assegnatari di una casella di posta elettronica con dominio aziendale ricordino che l'invio di una mail con il dominio aziendale comporta la responsabilità dell'azienda nei confronti dei terzi per tutto quanto è contenuto nella medesima.

Ciò premesso, i lavoratori non possono essere e non sono titolari di un diritto all'uso esclusivo della posta elettronica con dominio aziendale (**l'uso dell'iniziale del nome seguita dal cognome come indirizzo di e-mail non autorizza ad un uso privato ma all'uso per le funzioni aziendali ricoperte dal lavoratore**). In caso di assenza del lavoratore assegnatario, altri lavoratori o l'azienda possono, per motivi di lavoro, entrare nella sua casella e leggere i messaggi in entrata e in uscita.

L'azienda comunque accederà alla casella di posta elettronica - di cui sia titolare la medesima - utilizzata dal lavoratore solamente per motivi connessi con lo svolgimento del lavoro.

Pur ribadendo che è proibito l'uso privato della casella di posta aziendale, i lavoratori possono delegare un altro lavoratore ("fiduciario") a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Della delega al "fiduciario" deve essere informato il Responsabile della Sicurezza Informatica che svolgerà altrimenti direttamente o tramite suoi collaboratori l'attività dandone comunque comunicazione al lavoratore al momento del rientro in servizio insieme alla comunicazione della Password provvisoria utilizzata.

Qualunque lavoratore può rivolgersi al Responsabile della Sicurezza Informatica per richiedere informazioni su coma attivare una casella e-mail privata (ovviamente con dominio diverso da quello aziendale)

10. Obbligo di segretezza e responsabilità dei dati aziendali e personali

I lavoratori si impegnano a non divulgare a terzi estranei all'azienda dati e informazioni di cui vengano a conoscenza per motivi di lavoro. In particolare, essi si impegnano a mantenere il segreto e la massima riservatezza sull'anagrafe clienti, fornitori, contratti, documenti, progetti. Essi sono responsabili dell'uso non corretto di tali dati e informazioni.

Senza preventiva autorizzazione del Responsabile, non è possibile creare nuove ed autonome banche dati.

Nessun dato può essere trasmesso all'esterno in qualunque forma, sia come comunicazione che come diffusione, se non previa autorizzazione del titolare/responsabile.

11. Misure di sicurezza

Ogni incaricato è tenuto ad osservare in via generale le idonee misure di sicurezza volte a prevenire i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Anche al fine di conseguire un livello adeguato di sicurezza - secondo quanto previsto dall'Allegato B del D.Lgs. n. 196/2003 - è fatto inoltre obbligo di rispettare le prescrizioni dell'istruzione operativa "Prescrizioni per gli incaricati del trattamento dei dati" (già citata).

12. Gestione password

Ogni lavoratore deve proteggere il proprio computer tramite una password personale per rispondere ad un'esigenza di sicurezza nei rapporti con i propri colleghi e con i terzi.

Il lavoratore che opera con sistemi informatici non collegati alla rete aziendale ha il dovere di segnalare la propria password al

Responsabile dei Sistemi Informatici della propria area (es. Capo Cantiere) affinché altri possano accedere in sua assenza (per causa di: permessi, ferie, malattia, congedi, etc.) qualora l'accesso sia necessario per motivi di lavoro.

L'azienda si riserva comunque la facoltà di sostituire la password, qualora ciò sia necessario per motivi di lavoro.

13. Incarico per il trattamento dei dati

Il D.Lgs. 196/03, disciplina la gestione dei dati personali ed impone che all'interno di ogni realtà aziendale sia costituita una gerarchia, comprendente le figure del titolare, del responsabile e dell'incaricato, funzionale alla sua applicazione. Tale gerarchia non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate ai dipendenti.

Ogni singolo Impiegato è incaricato/a del trattamento di dati personali (dato che nell'ambito dello svolgimento delle proprie funzioni viene necessariamente a conoscenza dei contenuti delle banche dati presenti presso la propria unità operativa) nell'ambito delle mansioni ad esso assegnate. Le banche dati cui potrà accedere per il trattamento - previa abilitazione ed indicazione delle modalità di utilizzo - sono unicamente quelle previste per l'ufficio di appartenenza e descritte nelle apposite istruzioni del Sistema Qualità aziendale (sempre consultabili dal sito aziendale).

Per trattamento di dati deve intendersi: "operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"

L'accesso è in ogni caso consentito ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati. Pertanto, nella gestione dei dati dovrà osservare scrupolosamente le istruzioni impartite.

14. Prevenzione dell'accesso a determinati siti

Nella prospettiva della prevenzione di cui al presente documento, l'azienda si riserva la facoltà di adottare software volti a bloccare l'accesso a determinati siti a contenuto estraneo all'attività dell'azienda.

L'intervento sulle strutture aziendali con modalità automatiche di filtro e inibizione non comporta un controllo diretto o indiretto sulla posizione individuale, ma semplicemente può impedire l'accesso a determinati siti non funzionali all'attività aziendale, può impedire il downloading di materiale, funge da filtro per il virus detecting, impedisce l'invio o la ricezione di mail contenenti determinate parole (a sfondo sessuale o razzista) o di determinate dimensioni.

15. Cessazione del rapporto o modifica di funzione

A seguito della cessazione del rapporto o di modifica di funzione il Responsabile della Sicurezza Informatica potrà modificare la password assegnata al lavoratore senza più comunicarla allo stesso.

Per tutte le caselle che fanno riferimento al nome e cognome del lavoratore valgono le seguenti regole:

Per un anno la casella di posta precedentemente assegnata al lavoratore rimarrà attiva per la ricezione dei messaggi di interesse aziendale. Entro 2 mesi dalla modifica di funzione cessazione un messaggio di risposta automatica indicherà il nuovo indirizzo da utilizzare per raggiungere la funzione aziendale.

Il contenuto dei dati della casella personale ed il contenuto della posta aziendale del lavoratore rimarranno a disposizione dell'azienda che potrà darne l'accesso ad altri lavoratori per lo svolgimento delle attività aziendali per un periodo non superiore ai 10 anni (visto che potrebbero contenere dati aziendali necessari in caso di collaudi o contestazioni).

16. Smaltimento delle apparecchiature

L'azienda, anche al fine di prevenire la produzione di rifiuti di apparecchiature elettroniche, ne promuove il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantità da avviare allo smaltimento.

Questo comporta un rischio elevato di "circolazione" di componenti elettroniche che potrebbero contenere dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (l'azienda ha infatti deciso di non ricorrere alla cifratura dei dati per facilitare il recupero dei dati a fronte di malfunzionamenti).

L'azienda dovrebbe quindi adottare in occasione della dismissione di componenti elettronici suscettibili di memorizzare dati personali misure in grado di garantire l'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai dati personali memorizzati sul disco rigido dei *personal computer* o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica).

Il lavoratore che restituisce un'apparecchiatura (anche se non funzionante) dovrà informare circa la presenza di dati personali (normalmente non ammessi) per attivare le operazioni di cancellazione altrimenti non applicate ai singoli PC.

17. Segnalazioni all'Autorità Giudiziaria

Ogni utilizzo delle risorse informatiche aziendali da parte dei lavoratori tale da comportare una responsabilità anche penale dell'azienda verrà tempestivamente segnalato dall'azienda all'Autorità Giudiziaria senza che a tal fine sia necessaria una preventiva contestazione dell'addebito al lavoratore responsabile.

18. Responsabile della sicurezza informatica

Responsabile della sicurezza informatica è l'Ing. Giuliano Marullo (g.marullo@btpspa.it)

Il ruolo di Amministratori del sistema (con la possibilità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non sarebbero legittimati ad accedere rispetto ai profili di autorizzazione attribuiti) è affidato a società esterne il cui elenco aggiornato è possibile richiedere direttamente al Responsabile della sicurezza informatica.