REGOLAMENTO PER L'USO DEI SISTEMI INFORMATICI

(aggiornamento al Reg. UE 679/2016)

Approvato dal CdA in data 26 luglio 2023

Vi.abilità S.R.L.
Via Zamenhof, 829
36100 – Vicenza - Italy

Tel. +39 0444 385711
Pec: vi-abilita@legalmail.it
E – mail info@vi-abilita.it
Web site www.vi-abilita.it

Capitale sociale: 5.050.000,00 euro i.v.
Partita IVA: 02928200241
Registro Imprese di Vicenza: 02928200241
R:E:A: di Vicenza: n. 285329

SOMMARIO

Sommario

Art. 1 OGGETTO E FINALITÀ

1 Vi.abilità SRL procede regolarmente all'aggiornamento ed implementazione dei servizi Informatici e di Telecomunicazione (ICT) per la durata di un quinquennio al fine di consolidare e migliorare la qualità e l'affidabilità dei servizi offerti alla propria utenza. I temi oggetto di appalto ed esteriorizzazione dei servizi informatici (da ora in poi "Service Estermo") riguardano:
- servizi Intranet, con particolare riferimento ai servizi di Server Management, ai database, alla gestione della posta elettronica;
- fornitura dell'architettura e componenti hardware e software per le postazioni di lavoro presso la sede centrale di Vi.abilità S.r.l. e per la fonia fissa presso la sede centrale e presso gli uffici Tunnel Schio – Valdagno;
- servizi di Disaster recovery, backup e sicurezza;
- connettività;
- assistenza sistemistica ed helpdesk, con riferimento alla gestione delle richieste, alla sicurezza.

2 Il presente regolamento disciplina l'utilizzo di ogni sistema informatico all'interno della Società per una corretta ed adeguata gestione delle informazioni aziendali, affinché l'utilizzo degli strumenti informatici e telematici sia conforme alle finalità istituzionali e nel pieno rispetto della legge.

3 L'applicazione del presente regolamento garantisce il miglioramento materiale e immateriale delle condizioni di sicurezza funzionali alla protezione dei dati personali e patrimoniali.

4 I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti, o che si possono raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative, per la sicurezza del lavoro e per la tutela del patrimonio informativo della Società.

Art. 2 CAMPO DI APPLICAZIONE

1 Il regolamento si applica a tutti i dipendenti, senza distinzioni di ruolo e/o livello, nonché a tutti i collaboratori della Società a prescindere dal rapporto contrattuale in essere.

2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente/collaboratore in possesso di specifiche credenziali di autenticazione.
Tale figura potrà anche venir indicata come "autorizzato al trattamento".

Art. 3 PRINCIPI GENERALI E DI RISERVATEZZA NELLE COMUNICAZIONI

1 I principi a fondamento del presente regolamento sono quelli espressi nel "Regolamento Generale sulla Protezione dei Dati" n. 679/2016 unitamente a quanto previsto dalla Linea guida del Garante per l'uso della posta elettronica e Internet - 1 marzo 2007 [doc. web n. 1387522], dalla Linea guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico 14 giugno 2007 [doc. web n. 1417809] e precisamente:

- il principio di necessità: i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi in relazione alle finalità perseguite;
- il principio di correttezza: le caratteristiche essenziali dei trattamenti devono essere rese note ai dipendenti. Le tecnologie dell'informazione consentono di svolgere trattamenti ulteriori rispetti a quelli ordinariamente connessi all'attività lavorativa all'insaputa o senza la piena consapevolezza dei dipendenti; Vi.abilità s.r.l. pertanto favorisce la formazione continua di tutto il personale al fine di acquisire la necessaria consapevolezza nell'uso delle tecnologie informatiche e, più in generale, nel corretto utilizzo dei dati personali trattati per motivi di lavoro;
- principi di pertinenza e non eccedenza: i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime e nella misura meno invasiva possibile; le attività di

monitoraggio effettuate sui sistemi informatici devono essere svolte solo da soggetti preposti ed essere mirate all'ambito oggetto di rischio per la rilevazione di eventuali e possibili data breach.

2 Il personale deve attenersi alle seguenti regole:
- è vietato comunicare a soggetti non specificamente autorizzati i dati personali comuni, le particolari categorie di dati (rif. art. 9 Reg.UE 679/16), i dati giudiziari e quelli sanitari o altri dati, elementi e informazioni istituzionali dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie mansioni all'interno della Società. In caso di dubbio è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli mediante richiesta al responsabile del trattamento d'area;
- è vietata l'estrazione di originali e/o copie cartacee ed informatiche di documenti, fascicoli, lettere, data base, ecc. per uso personale;
- è vietato lasciare incustoditi documenti, fascicoli, ecc. che contengono dati personali e/o informazioni istituzionali quando il dipendente si allontana dalla postazione di lavoro;
- per le riunioni e gli incontri di particolare riservatezza dovranno essere utilizzate sale dedicate.

Si fa inoltre presente che:

1 L'Azienda individua le seguenti figure preposte inoltre alla progettazione ed esecuzione del contratto di servizi ed fornitura informatica ossia il personale incaricato formalmente alla gestione della infrastruttura informatica:
- RESPONSABILE SISTEMI INFORMATIVI: nella figura del Dirigente Area Tecnca in qualità di RUP del servizio esterno di "AGGIORNAMENTO ED IMPLEMENTAZIONE DEI SERVIZI INFORMATICI E DI TELECOMUNICAZIONE DI VI.ABILITA' S.R.L. "
- Direttore dell'Esecuzione del servizio esterni di "AGGIORNAMENTO ED IMPLEMENTAZIONE DEI SERVIZI INFORMATICI E DI TELECOMUNICAZIONE DI VI.ABILITA' S.R.L. "

2 L'amministratore del Sistema per la salvaguardia del patrimonio informativo ha stabilito una policy di navigazione di cui al cap. 10 del presente documento di cui un estratto è allegato al presente documento. La stessa policy potrà essere oggetto di continuo aggiornamento da parte del Rsponsabile sistemi informativi in relazione a quanto potrà emergere in materia nel corso dell'attività lavorativa
L'accesso alla rete, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo del lavoratore a distanza.

3 Il Titolare del trattamento ai sensi dell'art. 19 del presente Documento nonché il Responsabile Sistemi Informativi e il Direttore dell'Esecuzione di cui al precedente comma, nel rispetto delle regole, può effettuare verifiche a campione sugli strumenti informatici concessi in dotazione e/o sui server di rete per assicurare il corretto utilizzo dei dispositivi e dei programmi e applicazioni installati.

4 L'accesso al PC è protetto da un sistema di autenticazione. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza.
Non è consentita la copia o la trasmissione dei dati tramite dispositivi di memorizzazione, comunicazione o altro, se non con l'autorizzazione espressa dell'Amministratore del Sistema.

5 Al fine di non compromettere la sicurezza della Società e di prevenire conseguenze legali o di altro genere, gli utenti non dovranno scaricare software gratuiti (freeware) e shareware prelevati da siti Internet, se non espressamente autorizzati dall'Amministratore del Sistema.

Art. 4 LA RETE INFORMATICA

1 Il patrimonio informativo utilizza, per il trasporto dei dati, una piattaforma di Rete che, per il suo funzionamento, viene gestita internamente da personale debitamente individuato di cui all'art. 3 del presente Regolamento oltre che da un Service Esterno (individuato allo scopo da specifico contratto di servizio) a cui viene demandata la regolare verifica di gestione ed efficienza.

Si elencano di seguito alcune prescrizioni operative:

- le unità di Rete sono aree/spazi di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi; pertanto qualunque file non riconducibile all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; su queste vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema;
- l'accesso alle diverse unità di Rete è possibile mediante l'uso di un PC aziendale formalmente consegnato a ciascun dipendente e personalizzato in funzione dell'ufficio di competenza e definito all'atto della creazione del profilo utente assegnato al dipendente;
- ogni utilizzatore di unità di Rete, con frequenza periodica di almeno tre mesi, dovrà effettuare la pulizia dei propri archivi evitando la presenza di files obsoleti o inutili; particolare attenzione deve essere prestata alla duplicazione dei dati: è assolutamente da evitare un'archiviazione ridondante;
- la stampa in Rete di documenti con dati personali e sensibili per evitare la diffusione di notizie, documenti ecc.. , dovrà avvenire mediante l'impiego della funzione di "Stampa Riservata" disponibile nell proprietà di stampa di ciascuna stampante di rete configurata;
- per l'accesso al proprio PC ciascun utente deve essere in possesso della specifica credenziale di autenticazione di cui al cap. 5 del presente regolamento;
- è assolutamente proibito autenticarsi sul proprio PC assegnato con le credenziali di altro utente salva la formale autorizzazione di quest'ultimo resa anche all'Amministratore di sistema a mezzo e-mail;
- le credenziali di accesso alla rete ed ai programmi installati sul singolo PC sono segrete e vanno comunicate e gestite secondo le procedure impartite;
- si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio automatico; la responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente;
- il personale addetto alla gestione della Rete può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di Rete.

Art. 5 GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

1 A ciascun dipendente è formalmente consegnata l'attrezzatura informatica di lavoro qui trattata mediante specifico verbale sottoscritto dal dipendente per accettazione. All'atto di consegna il PC stesso sarà configurato sul singolo utente in funzione del ruolo aziendale ricoperto. Il profilo configurato è personale e personalizzato; le credenziali di autenticazione per l'accesso alla Rete vengono assegnate con formale richiesta del responsabile d'area nell'ambito del quale la risorsa andrà ad operare come NUOVO UTENTE.
Nel caso di collaboratori la preventiva richiesta verrà inoltrata direttamente dal responsabile d'area con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà venir custodita dall'autorizzato al trattamento con la massima diligenza e non divulgata. Non è consentita la modifica della password di accensione (BIOS).

3 La parola chiave (formata da lettere maiuscole o minuscole e/o numeri, anche in combinazione fra loro) deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'Autorizzato al trattamento. A ciascun utente sarà richiesto automaticamente ogni 90 giorni la modifica della propria Password di accesso.
Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale dedicato.

Art. 6 UTILIZZO APPARECCHIATURE INFORMATICHE (personal computer, personal computer portatile, tablet)

1 La Società favorisce la piena connettività in Rete Intranet ed Internet dei dipendenti /collaboratori tuttavia ogni utente dovrà attenersi alle seguenti prescrizioni:

- l'apparecchiatura affidata al dipendente è uno strumento di lavoro; ogni utilizzo non inerente all'attività lavorativa può contribuire a creare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza patrimoniale;
- l'utilizzo del PC o di ogni altro mezzo di elaborazione dati per scopi personali dai quali l'utilizzatore tragga o meno un vantaggio economico personale può rappresentare un uso indebito dello strumento di lavoro per il quale possono applicarsi le previste sanzioni disciplinari o contrattuali nel caso di terzi;
- il bene deve essere custodito con cura evitando ogni possibile forma di danneggiamento;
- l'accesso al PC, alle applicazioni con dati sensibili, patrimoniali, personali, per l'uso d'internet, è subordinato all'adozione di idonea password conosciuta e custodita dall'Autorizzato al trattamento con la massima diligenza e non divulgata;
- evitare l'installazione autonoma di programmi provenienti dall'esterno;
- evitare l'uso di programmi diversi da quelli distribuiti ufficialmente;
- evitare la modifica delle caratteristiche software e hardware predisposte per il proprio PC, salvo autorizzazione esplicita dell'Amministratore del Sistema;
- chiudere correttamente ogni sessione aperta e successivamente spegnere il proprio PC prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio;
- prima di lasciare incustodito il proprio PC utilizzare l'apposita password con lo screen saver chiudendo preventivamente l'abilitazione alle applicazioni (ad esempio Crtl+Alt+Canc per Windows);
- il personale incaricato formalmente alla gestione della infrastruttura informatica, per l'espletamento delle sue funzioni, per garantire la sicurezza del sistema informatico e per garantire la regolarità del servizio del lavoro, ha la facoltà, in qualunque momento, e su disposizione del Titolare del trattamento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica LIMITATAMENTE alla casella di posta comune; analoghe verifiche possono essere effettuate sui siti internet visitati dagli utenti abilitati alla navigazione esterna; l'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo del lavoratore a distanza;
- non è consentito l'uso di programmi diversi da quelli ufficialmente installati, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti; inosservanza della presente disposizione espone la Società a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software vengono sanzionate anche penalmente essendo a carico della Società le sanzioni amministrative elevate in caso di accertamento d'illecito;
- il personale Autorizzato al servizio di gestione della Rete ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.; l'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico;
- non è consentito l'accesso contemporaneo con lo stesso account da più PC;
- segnalare immediatamente all'Amministratore del Sistema l'eventuale presenza di virus informatici ed ogni altra anomalia riscontrata;

- è vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica su aree di Rete o singolo PC.

Art. 7 UTILIZZO DI PC PORTATILI

1 L'utente è responsabile del PC portatile e di ogni altra attrezzatura assegnatagli, e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in Rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

2 Tali strumenti devono essere usati esclusivamente per le finalità connesse all'esecuzione della prestazione lavorativa. È espressamente vietato ogni utilizzo del sistema informatico per finalità diverse da quelle strettamente professionali.

3 Il PC portatile non potrà essere ceduto a terzi ad alcun titolo, neanche temporaneamente.
L'assegnatario è responsabile dell'utilizzo e della custodia del PC portatile e dei relativi accessori secondo l'ordinaria diligenza.

Art. 8 UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.) contenenti dati sensibili, nonché informazioni costituenti know-how, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale addetto e seguire le istruzioni da questo impartite. In ogni caso, tali supporti magnetici devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

2 È vietato l'utilizzo di supporti rimovibili personali sulla rete ed apparecchiature di lavoro. L'Azienda fornisce a ciascun dipendente a cui è assegnata una postazione di lavoro, una chiavette USB di cui sarà pienamente responsabile e che dovrà essere restituita alla conclusione del rapporto lavorativo. L'utente è responsabile della custodia dei supporti di memorizzazione e dei dati in essi contenuti.

3 Tutti i supporti USB (di memoria) prima di essere utilizzati all'interno del sistema, devono essere necessariamente validati dall'Amministratore di Sistema.
Non è consentito:
   - l'utilizzo, non autorizzato, di supporti di memoria di provenienza ignota (chiavette USB, hard disk esterni, CD-ROM, DVD, ecc.);
   - scaricare nella Rete della Società files non aventi alcuna attinenza con la propria prestazione lavorativa.

   Da evitare:
   - la copia su supporti portatili di memorizzazione di particolari categorie di dati - ex sensibili (rif. articolo 9 del Reg.UE 679/16) per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi ovvero il cosiddetto data breach;

4 Qualora il contenuto del supporto di memorizzazione (o memoria USB) debba essere copiato su un hard disk locale od altro strumento elettronico di trattamento, accertarsi di cancellare il relativo contenuto al termine dell'operazione di trattamento.

5 Prestare particolare attenzione affinché nessun dato rimanga nella memoria buffer, nella clipboard, negli appunti o all'interno del cestino, in sistemi operativi di tipo Windows.

6 I supporti DVD, CD-ROM ecc., qualora contengano dati personali, devono essere trattati (protetti o cifrati) per evitare l'eventuale recupero dei dati da parte di soggetti non autorizzati. In particolare, se

contenenti particolari categorie di dati, devono essere custoditi in contenitori ovvero in archivi chiusi a chiave.

È altresì opportuno:

- evitare di lasciare incustoditi i supporti di memorizzazione, anche per breve periodo, poiché gli stessi possono essere rapidamente letti e copiati;
- identificare ogni supporto di memorizzazione, per evitare di confonderli e generare un possibile data breach;
- proteggere con apposite buste o contenitori, che ne dimostrino l'effrazione, i supporti di memorizzazione spediti o consegnati a terzi;
- in caso di alienazione provvedere alla distruzione rigando la superficie per poi spezzarli.

Art. 9 UTILIZZO DELLA POSTA ELETTRONICA

1 Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni, per le finalità della Società ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente o collaboratore che utilizza tale funzionalità. Non è possibile utilizzare tale servizio per finalità in contrasto con quelle di Vi.abilità s.r.l. o non pertinenti all'attività lavorativa.

2 Ad ogni utente viene fornito un account e-mail nominativo. L'utente cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa. Vi.abilità s.r.l. fornisce inoltre delle caselle di posta elettronica associate a ciascuna unità organizzativa/ufficio da utilizzare preferibilmente quando le comunicazioni sono di interesse collettivo, al fine di evitare che utenti singoli mantengano l'esclusività su dati della Società. Agli utenti autorizzati all'uso di suddette caselle di posta non nominative la casella di posta elettronica verrà configurata sul proprio PC ed associata al proprio profilo utente personalizzato.

3 Al fine di prevenire conseguenze legali o di altro genere, gli utenti dovranno adottare i seguenti comportamenti:

- se, nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi), evitare di aprirle (in particolare se contenenti allegati .exe o .pdf), e procedere all'inoltro (come allegato senza aprirle) all'Amministratore del Sistema;
- non utilizzare le caselle di posta elettronica per l'invio di messaggi personali, salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

4 È vietato utilizzare le "caselle di posta elettronica nominali", cioè inizialenomecognome@vi.abilita.it per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale addetto. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

È obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

5 Per inviare a destinatari esterni messaggi contenenti allegati con dati personali terzi è obbligatorio che questi allegati vengano preventivamente resi inintelligibili, se del caso, attraverso criptazione con apposito software. La password di criptazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail. Tutte le informazioni istituzionali e i dati personali di competenza possono essere inviati soltanto a destinatari qualificati e competenti, individuati nel Registro dei trattamenti.

Valutare come cambiarla

Art. 10 NAVIGAZIONE IN INTERNET

1 Il computer (fisso o mobile) assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile per lo svolgimento della propria attività lavorativa. E' consentita la navigazione in internet nei limiti della correttezza. L'amministratore del Sistema ha stabilito una policy di navigazione in base agli ip sorgenti in funzione delle categorie con cui il firewall cataloga i diversi siti internet. Estratto della stessa è allegata al presente regolamento e potrà essere oggetto di aggiornamento qualora rilevato necessario in rapporto alla sicurezza informativa del sistema dal Responsabile Servizio Informativo. Nello specifico sulla scorta della categoria di appartenenza l'accesso ad una determinata pagina web può essere posto in:
Block (bloccato con log);
Allow (consentito senza log),
Monitor (consentito con log);
Warning (consentito con messaggio: il Firewall presenta una pagina che dice che la pagina che si vuole consultare non è compliant e ha un tempo limitato per poterla vedere di base 5 min).

2 All'utente non è consentito comunque l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;

Art. 11 UTILIZZO DEI TELEFONI, SMARTPHONES E FOTOCOPIATRICI

1 Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, e quindi non sono consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza.

2 L'utente è responsabile dell'utilizzo e della custodia del cellulare istituzionale assegnato. È vietata l'installazione e l'utilizzo di applicazioni che possano arrecare danni al dispositivo stesso o compromettere la sicurezza dello stesso. Ai cellulari e smartphone della Società (di servizio) si applicano le medesime regole previste per gli altri dispositivi informatici per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica e la corretta navigazione in internet.

3 È vietato l'utilizzo delle fotocopiatrici per fini personali, salva diversa esplicita autorizzazione da parte del responsabile dell'area.

4 Per quanto riguarda l'uso delle stampanti gli utenti sono tenuti a:

- stampare i documenti solo se strettamente necessari allo svolgimento della propria attività;
- utilizzare preferibilmente le stampanti di rete condivise rispetto a quelle locali/personali, per ridurre il consumo di materiali (toner, ecc.);
- stampare in bianco/nero e fronte/retro per ridurre i costi.

La stampa in Rete di documenti con dati personali e sensibili per evitare la diffusione di notizie, documenti ecc.. , dovrà avvenire mediante l'impiego della funzione di "Stampa Riservata" disponibile nell proprietà di stampa di ciascuna stampante di rete configurata;

Art. 12 PROTEZIONE ANTIVIRUS

Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale preposto alla gestione dei Sistemi Informatici.

Ogni dispositivo di memoria di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso in cui venga rilevato un virus, dovrà essere prontamente consegnato al personale preposto alla gestione dei Sistemi Informatici.

L'uso di un dispositivo USB di memoria deve essere comunque autorizzato dall'Amministratore del Sistema per evitare di danneggiare la rete.

1 Si elencano di seguito alcune regole generali di comportamento (legate ad esempio all'uso della posta elettronica) che devono essere sempre seguite per ridurre al minimo il rischio di infezioni da virus informatici che comprometterebbero l'integrità del patrimonio informativo:

- evitare di aprire allegati alle e-mail direttamente dal programma di posta; è preferibile procedere al salvataggio dell'allegato su una cartella locale permettendo così di verificarne l'effettiva "estensione" (un file di testo .TXT potrebbe mascherare un file .TXT.vbs dannoso); alcuni virus/worm si diffondono, infatti, utilizzando una doppia estensione finale; ad esempio il file "pippo.txt.exe" non è un file di testo (.txt), ma un file eseguibile (.exe); un allegato del genere non va mai aperto o salvato, va cancellata immediatamente l'e-mail e, successivamente, svuotata la cartella "Posta eliminata";
- qualora, senza l'intervento dell'utente, durante l'anteprima dell'e-mail, appaia una finestra del client di posta che avverte se aprire o salvare l'allegato, annullare la richiesta e cancellare l'e-mail; alcuni virus/worm sono in grado di "forzare" l'utente ad aprire l'allegato;
- non aprire mai file eseguibili o dal contenuto attivo (con estensione .exe, .pif, .com, .vbs, .bat, .cmd, .dot, .reg, .js, .scr, .xlm, .wmz, .jar, .html,);
- non fare eccezioni anche se il mittente è una persona conosciuta e fidata in quanto, a volte, i virus si "impossessano" della casella e-mail e/o della rubrica di un utente e inviano e-mail infette in maniera "autonoma"; a volte i virus sono in grado di falsificare anche il mittente dell'e-mail, pertanto si potrebbero ricevere e-mail da falsi sistemi automatici antivirus che ci informano di essere infetti; nella maggior parte dei casi si tratta di un falso allarme; in tale circostanza è opportuno verificare che l'antivirus sia correttamente funzionante;
- diffidare sempre delle e-mail inviate da mittenti sconosciuti o che inviano allegati non attesi o da offerte gratuite di software, immagini, password di accesso a siti, o altri beni;
- limitare l'iscrizione a forum, newsgroup e liste di distribuzione pubbliche, in modo da non diffondere, ove non necessario, il proprio indirizzo e-mail (utilizzare pertanto lo strumento elettronico in conformità con quanto indicato nelle lettere di incarico al trattamento dei dati); tale raccomandazione è anche una valida strategia di difesa contro il fenomeno dello "spamming", cioè l'invio massivo di e-mail pubblicitarie o dai contenuti offensivi e illegali.

Art. 13 ASSISTENZA AGLI UTENTI E MANUTENZIONI

1 L'assistenza sistemistica ed helpdesk, qualora gli utenti ne abbiano necessità o per ragioni generiche di sicurezza, è demandata a service estermo. L'inoltro della richiesta di intervento dovrà rivolgersi in primis al Direttore dell'Esecuzione del Servizio o in sua assenza inoltrando una e-mail al **supporto del service esterno** descrivendo il problema e fornendo sempre uno screen shot (copia schermata video) di eventuali messaggi d'errore.

2 L'Amministratore del Sistema, in base alla tipologia dell'intervento richiesto, può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per:
- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

3 Quando l'intervento richiede l'accesso alle cartelle di rete personali dell'utente mappata con la lettera J o specificatamente al profilo utente , è necessario il consenso del dipendente/collaboratore. In caso di sua assenza o impossibilità di contattarlo, L'amministratore del Sistema potrà procedere al reset della Password di accesso per garantire la continuità operativa del servizio procedendo successivamente alla formale comunicazione a mezzo email all'utente stesso dell'avvenuta modifica delle credenziali di accesso. Al successivo nuovo accesso da parte dell'utente al proprio PC, lo stesso è tenuto scrupolosamente all'aggiornamento della Password. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante le credenziali dell'utente, l'Amministratore del Sistema è autorizzato ad effettuarlo senza il consenso del dipendente/collaboratore cui la risorsa è assegnata.

4 L'assistenza da remoto sui PC della rete da parte di terzi (fornitori di programmi) deve essere autorizzato dall'Amministratore del Sistema per le verifiche della modalità di intervento per il primo accesso. Le richieste successive possono essere gestite autonomamente dall'utente finale se effettuate con la medesima modalità. Durante questi interventi l'utente richiedente o l'Amministratore di Sistema devono presenziare in modo da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

Art. 14 ACCESSO AI DATI TRATTATI DALL'UTENTE

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è data facoltà al Titolare del trattamento, sentita l'effettiva necessità espressa dal Responsabile del trattamento, di accedere direttamente, nel rispetto della normativa sulla privacy e dei diritti dei lavoratori, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico generato unicamente per garantire il funzionamento dei processi amministrative della Società.

Art. 15 CONTROLLI SUGLI STRUMENTI

1 In caso di anomalie, il personale incaricato effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.
Le dotazioni di cui al presente Regolamento sono strumenti di lavoro e, pertanto, rientrano nella disciplina dell'art.23 comma 2 del Decreto legislativo n. 151/2015. Le attività di controllo saranno effettuate sul presupposto di tutela del patrimonio e della sicurezza informatica.

2 Vi.abilità s.r.l. può verificare, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro può avvalersi, nel rispetto dello Statuto dei lavoratori di sistemi di controllo che consentono indirettamente il controllo e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. I controlli devono essere effettuati nel rispetto del presente regolamento.

3 L'introduzione o la modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati devono rispettare le procedure di informazione e di consultazione dei lavoratori e dei sindacati.

Il Titolare del trattamento ha il potere di svolgere attività di monitoraggio che viene realizzata dall'Amministratore del Sistema, o da personale delegato, nel rispetto della normativa citata e dei seguenti principi:

- proporzionalità: il controllo deve essere adeguato, pertinente e non eccessivo rispetto alle finalità perseguite;
- trasparenza;
- pertinenza e non eccedenza: il controllo deve evitare una interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, e non deve essere prolungato, costante o indiscriminato.

4 L'utilizzo degli strumenti informatici della Società può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali del dipendente/collaboratore, sono oggetto di controllo da parte di Vi.abilità s.r.l., per il tramite dell'Amministratore del Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e la tutela del patrimonio, per la sicurezza e la salvaguardia del sistema informatico. Gli interventi di controllo sono di tre tipi e seguiranno i seguenti iter:

a) controlli per la tutela del patrimonio, la sicurezza e la salvaguardia del sistema informatico: se per l'attività di controllo è necessario l'accesso agli strumenti, alle risorse informatiche e relative informazioni, il Responsabile del trattamento, per il tramite dell'Amministratore del Sistema, deve seguire questo iter:

- avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo al rispetto del regolamento:
- se il comportamento anomalo persiste, dopo almeno 7 giorni, la Società può autorizzare l'Amministratore del Sistema ad accedere alle informazioni con possibilità di rilevare i files trattati, siti web visitati, documenti scaricati, software installati, ecc., durante l'attività lavorativa. Tale attività può essere effettuata in forma anonima o tramite controllo del numero IP, dell'utente e del soggetto che non osserva le istruzioni impartite;
- se il rischio di compromissione del sistema informativo aziendale è imminente e grave il Responsabile del trattamento, unitamente all'Amministratore del Sistema, interviene sullo strumento da cui proviene la minaccia bloccandolo.

b) controlli per esigenze produttive e di organizzazione: qualora si verifica l'urgente e improrogabile necessità di accedere a files o informazioni lavorative disponibili su risorse informatiche di un dipendente/collaboratore non reperibile (per assenza temporanea o cessazione dal servizio), il Responsabile del trattamento autorizza l'accesso, per il tramite dell'Amministratore del Sistema, garantendo:

- accesso limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro; eventuali files o informazioni personali sono utilizzabili a tutti i fini connessi al rapporto di lavoro, ai sensi di quanto disposto dal successivo articolo;
- documentare l'attività svolta al Titolare del trattamento.

c) controlli per la verifica o la prevenzione delle commissione di possibili reati:

- atto del Titolare del trattamento o del Direttore Generale che attesti le necessità di accesso allo strumento;
- incarico all'Amministratore del Sistema di accedere alla risorsa con credenziali di "Amministratore" avvalendosi se nel caso del Service esterno avendo cura di non alterare elementi idonei alla alla rilevanza del reato. Della sola attività di accesso alla postazione di lavoro con credenziali di "Amministratore" dovrà essere dato avviso all'utente senza ulteriore specificazione;

Art. 16 SANZIONI DISCIPLINARI

1 È fatto obbligo a tutti i dipendenti/collaboratori di osservare le disposizioni del presente regolamento. Eventuali violazioni del regolamento o di altre norme comportano, a seconda della gravità dell'infrazione, l'adozione dei provvedimenti disciplinari nelle sue varie forme.
2 Vi.abilità s.r.l. si riserva il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di danni alla Società.

Art. 17 UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEGLI AMMINISTRATORI

1 Gli amministratori che utilizzano le risorse informatiche della Società per l'espletamento delle funzioni connesse al proprio mandato, sono tenuti all'osservanza del regolamento.

Art. 18 TRATTAMENTO DEI DATI PERSONALI (INFORMATIVA EX ARTT. 13 E 14 DEL REGOLAMENTO UE 2016/679)

1 Titolare del trattamento dei dati personali ai sensi dell'art. 44 del CSDP del servizio esterno denominato :"AGGIORNAMENTO ED IMPLEMENTAZIONE DEI SERVIZI INFORMATICI E DI TELECOMUNICAZIONE DI VI.ABILITA' S.R.L. " è l'Appaltatore del Servizio Esterno stesso nella persona individuato all'atto di sottoscrizione del contratto d'appalto.
2 I dati personali dei dipendenti sono trattati in ragione del rapporto di lavoro instaurato. Nell'ambito di tali finalità il trattamento riguarda anche i dati relativi alle registrazioni e alla creazione di credenziali di accesso a portali informativi necessari per la gestione del rapporto di lavoro. Non è previsto l'uso di trattamenti automatizzati o processi decisionali automatizzati o volti a profilare il dipendente da parte del. Le categorie dei dati trattati sono riportate nel Registro dei Trattamenti disponibile presso la sede della Società.
3 Il presente regolamento costituisce adeguata informazione delle modalità d'uso dei sistemi, applicazioni e strumenti informatici della Società nel rispetto di quanto disposto quali misure di sicurezza di cui all'articolo 32 del Regolamento UE n. 679/2016

Art. 19 ENTRATA IN VIGORE DEL REGOLAMENTO

1 Il presente regolamento entra in vigore con l'avvenuta approvazione da parte del Consiglio di Amministrazione della Società.
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia devono intendersi abrogate e sostituite dalle presenti.
Il regolamento è messo a disposizione di ciascun dipendente mediante trasmissione per posta elettronica interna ed è pubblicato sul sito web di Vi.abilità s.r.l. alla sezione "Amministrazione trasparente" - sottosezione "Atti generali".

Art. 20 ALLEGATI

Tabelle di policy di navigazione in base agli IP sorgenti in funzione delle categorie con cui il firewall cataloga i diversi siti internet.

TABELLE DI POLICY DI NAVIGAZIONE

Potentially Liable 9	
Drug Abuse	Allow
Hacking	Allow
Illegal or Unethical	Allow
Discrimination	Allow
Explicit Violence	Allow
Extremist Groups	Block
Proxy Avoidance	Allow
Plagiarism	Allow
Child Abuse	Block
Adult/Mature Content 15	
Alternative Beliefs	Block
Abortion	Block
Other Adult Materials	Block
Advocacy Organizations	Block
Gambling	Block
Nudity and Risque	Block
Pornography	Block
Dating	Block
Weapons (Sales)	Block
Marijuana	Block
Sex Education	Block
Alcohol	Block
Tobacco	Block
Lingerie and Swimsuit	Block
Sports Hunting and War Games	Block
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow

Security Risk 6	
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Monitor
Newly Observed Domain	Monitor
Newly Registered Domain	Monitor
General Interest - Personal 35	
Advertising	Allow
Brokerage and Trading	Allow
Games	Allow
Web-based Email	Allow
Entertainment	Allow
Arts and Culture	Allow
Education	Allow
Health and Wellness	Allow
Job Search	Allow
Medicine	Allow
News and Media	Allow
Social Networking	Allow
Political Organizations	Allow

45% 89

54% 89

General Interest - Personal 35	
Reference	Allow
Global Religion	Allow
Shopping	Allow
Society and Lifestyles	Allow
Sports	Allow
Travel	Allow
Personal Vehicles	Allow
Dynamic Content	Allow
Meaningless Content	Allow
Folklore	Allow

General Interest - Personal 35	
Web Chat	Allow
Instant Messaging	Allow
Newsgroups and Message Boards	Allow
Digital Postcards	Allow
Child Education	Allow
Real Estate	Allow
Restaurant and Dining	Allow
Personal Websites and Blogs	Allow
Content Servers	Allow
Domain Parking	Allow

Web Chat	Allow
Instant Messaging	Allow
Newsgroups and Message Boards	Allow
Digital Postcards	Allow
Child Education	Allow
Real Estate	Allow
Restaurant and Dining	Allow
Personal Websites and Blogs	Allow
Content Servers	Allow
Domain Parking	Allow

General Interest - Personal 35	
Armed Forces	Allow
Web Hosting	Allow
Secure Websites	Allow
Web-based Applications	Allow
Charitable Organizations	Allow
Remote Access	Allow
Web Analytics	Allow
Online Meeting	Allow
Unrated 1	94% 89
Unrated	Block