C O M U N E D I O L B I A

Settore AA.GG. e Provveditorato - Servizio ITC

Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione Internet, della gestione della posta elettronica nonché della gestione dei documenti analogici del Comune di Olbia

Nr. Revisione	Descrizione Modifiche	Data
0	Prima Stesura	01/08/2018
1	Revisione	20/05/2020

Approvato dalla Giunta comunale con delibera n.110 del 26/05/2020

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

DISCIPLINARE INTERNO SULLE NORME COMPORTAMENTALI PER L'ACCESSO AI SISTEMI ED ALLE RISORSE INFORMATICHE, PER LA GESTIONE DELLA NAVIGAZIONE IN INTERNET E DELLA POSTA ELETTRONICA DELL'ENTE NONCHE' DELLA GESTIONE DEI DOCUMENTI ANALOGICI.

Il presente documento ha per oggetto i criteri e le modalità operative per l'accesso ai sistemi ed alle risorse informatiche, per la gestione della navigazione in Internet e della posta elettronica da parte dei dipendenti del Comune di Olbia e di tutti gli altri soggetti autorizzati che, a vario titolo, prestano servizio o attività per conto e nelle strutture dell'Amministrazione comunale (Titolare del trattamento).
Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o categoria, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione.
Il presente documento integra le istruzioni impartite dal Titolare in sede di designazione degli incaricati e sostituisce ogni precedente indicazione impartita in materia.

L'utente è responsabile di qualsiasi danno arrecato al Titolare, sia esso patrimoniale che non patrimoniale, e/o a terzi in violazione di quanto espressamente previsto dalla normativa e di quanto indicato nel presente disciplinare. La violazione delle presenti disposizioni può comportare anche l'applicazione delle sanzioni disciplinari rimanendo ferma ogni ulteriore forma di responsabilità penale.

Di seguito, vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte, che anche inconsapevolmente, potrebbero comportare rischi alla sicurezza dei dati, documenti e archivi.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

1. UTILIZZO DELLE POSTAZIONE DI LAVORO IN SEDE O IN SMART WORKING, SISTEMI PORTATILI, STAMPANTI E TELEFONIA FISSA.

1.1 La postazione di lavoro affidata al dipendente deve essere utilizzata strettamente per attività lavorative ed ogni utilizzo differente può contribuire a creare dei disservizi; inoltre, potrebbe insinuare minacce alla sicurezza dei Dati trattati dal Titolare. Tutti i dipendenti devono custodire la propria postazione di lavoro in modo diligente, segnalando per tempo ogni anomalia riscontrata e/o guasto al proprio responsabile o all'ufficio Sistemi Informativi.

1.2 L'accesso a ciascuna postazione è protetto da credenziali di autenticazione che risiedono sul Server di Dominio: tali credenziali sono costituite da "userID" e "password", e sono conosciute esclusivamente dall'utente.

1.3 Le credenziali di autenticazione devono essere gestite attenendosi alle seguenti istruzioni:

1.3.1 La password deve essere costituita da almeno otto caratteri alfanumerici di cui almeno tre differenti (scelti tra lettere minuscole, maiuscole, numeri e caratteri speciali)

1.3.2 La password deve essere autonomamente sostituita dall'utente (policy impostata lato Server di Dominio) al primo utilizzo e successivamente modificata ogni qual volta sia richiesto dal sistema.

1.3.3 La password non deve contenere riferimenti diretti o indiretti agevolmente riconducibili all'utente stesso.

1.3.4 Le password (anche quelle degli applicativi, i PIN e/o qualsiasi altro codice di protezione) devono essere custodite con la massima attenzione e segretezza (non devono mai essere scritte su fogli o biglietti che vengono lasciati in prossimità del dispositivo) e non devono essere divulgate o comunicate a terzi per nessuna ragione. Saranno passibili di provvedimenti i metodi "non standard" quali post-it, calendari e qualsiasi altro mezzo non idoneo di custodia, che potrà agevolare un uso illecito delle credenziali.

1.3.5 L'utente è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.

1.3.6 Le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise con altri utenti. Se un utente necessita di trattare gli stessi Dati e/o le stesse procedure dovrà richiedere, delle credenziali personali, al titolare del trattamento che a sua volta le chiederà all'Amministratore di Sistema, persona autorizzata a creare le dovute credenziali di autenticazione necessarie.È fatto divieto di comunicare la password per telefono o altro mezzo a soggetti che si presentano come colleghi, tecnici e supervisori.

1.4 Il dipendente preso atto che, la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai Dati cui il medesimo è abilitato, con possibilità di gestione degli stessi, si impegna a:

1.4.1 Non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;

1.4.2 Non utilizzare credenziali (user ID e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti a conoscenza casualmente;

1.4.3 Mantenere la corretta configurazione del proprio PC non alterando le componenti hardware e software predisposte, né tanto meno installando dei software non autorizzati.

1.5 Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

1.6 Non rispondere a messaggi di posta elettronica che richiedano la verifica delle proprie credenziali di accesso ai servizi finanziari (banche o altri istituti finanziari).

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

1.7 Ogni postazione di lavoro dovrà essere bloccata in caso di non utilizzo o di assenza temporanea, tramite blocco manuale o salvaschermo con richiesta di password al riavvio. Sarà compito del dipendente procedere a tale blocco.
L'Amministratore di Sistema, in ogni caso, imposterà un tempo di 20 minuti come blocco automatico su tutte le postazioni di lavoro.
1.8 In caso di assenza prolungata nel corso della giornata, è fatto obbligo di chiudere le applicazioni aperte dalle quali si ha accesso ai dati personali.
1.9 Spegnere sempre la propria postazione ed i relativi dispositivi ad essa connessi al termine dell'orario di lavoro.
1.10 Non è consentito installare/eseguire autonomamente software provenienti dall'esterno senza la preventiva autorizzazione dell'Amministratore di Sistema.
1.11 Nel caso di necessità di acquisto di programmi, di applicativi e procedure di pertinenza esclusiva di uno o più Servizi, sarà necessaria l'autorizzazione preventiva da parte dell'Amministratore di Sistema.
1.12 Non è consentito ai dipendenti modificare le impostazioni sulla scheda di rete LAN e neppure sul browser di navigazione, salvo esplicita autorizzazione dell'Amministratore di Sistema.
1.13 Non è assolutamente consentito l'uso/l'installazione sul proprio PC di dispositivi, neanche personali, di memorizzazione (HardDisk Esterni, chiavette USB, ecc), comunicazione o altro (masterizzatore, ecc) se non previa espressa autorizzazione dell'AdS a seguito di scritta da parte del Dirigente del Servizio cui è assegnato il dispositivo.
1.14 In caso di autorizzazione all'utilizzo di supporti di memorizzazione, gli stessi dovranno essere di proprietà del Titolare e andranno criptati.
1.15 Ogni dipendente deve comunque prestare la massima attenzione ai supporti di memorizzazione di origine esterna onde evitare di scaricare, anche inconsapevolmente, virus e/o qualunque codice maligno. Per tale motivo ogni supporto deve preventivamente essere sottoposto ad una analisi dell'Antivirus Endpoint in dotazione dell'Ente e condervata una copia dell'esito della scansione.
1.16 È assolutamente vietato copiare, scaricare e mettere a disposizione di altri materiale protetto da copyright (file musicali, filmati, ecc) di cui il Titolare non abbia acquisito i diritti.
1.17 Oltre alle postazioni di lavoro fisse, ogni dipendente autorizzato all'utilizzo di apparecchiature portatili di proprietà del Titolare quali notebook, tablet e smartphone dovrà prenderne particolare cura; le stesse andranno messe in sicurezza creando blocchi di sistema (es: pin, blocco schermo sequenza, sistemi biometrici). L'utente si impegna ad utilizzarle unicamente in prima persona ed infine a restituirle, quando richieste, in buono stato d'uso. In casi smarrimento/perdita di possesso si obbliga ad avvisare tempestivamente (entro 12 ore), in forma scritta, il Titolare del Trattamento e l'Amministratore di Sistema. L'assegnatario si impegna, altresì, a non effettuare alcuna attività illecita per mezzo del bene consegnato ed in particolare: non eseguirà manomissioni fisiche dei dispositivi, non installerà e non accederà a file, materiali, siti o contenuti illeciti ai sensi delle vigenti norme o comunque tutelati dal diritto d'autore senza le necessarie licenze.
1.18 In caso di utilizzo di dispositivi personali, si richiede che anche questi vengano protetti ed in caso di smarrimento/vendita o altra perdita di possesso, si avvisi preventivamente o tempestivamente (entro 24 ore), in forma scritta, il Titolare del Trattamento, l'Amministratore di Sistema ed il Responsabile della protezione dei dati personali nominato dal Comune.
1.19 Le stampanti verranno installate per gruppi di lavoro, tramite policy di dominio. Per finalizzare la procedura di stampa, andrà inserito un PIN personale al momento del ritiro dei fogli stampati.
1.20 Gli scanner degli apparati multifunzione verranno configurati per poter scansionare in cartelle di rete, legate ai gruppi di lavoro. Sarà cura dell'utente cancellare, dalla cartella condivisa, i documenti scansionati una volta verificata l'attività di scansione.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

1.21 Il telefono aziendale (fisso e/o portatile) affidato all'utente è uno strumento di lavoro. L'uso del telefono è consentito esclusivamente per lo svolgimento dell'attività lavorativa, non sono consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

1.21.1 La ricezione o l'effettuazione di telefonate personali mediante utilizzo del telefono fisso aziendale è consentito solo nel caso di comprovata necessità ed urgenza. Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere messaggi di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, salvo diverse disposizioni aziendali.

1.21.2 Non sono soggetti a tale disciplina i telefoni cellulari concessi dall'Ente in "uso promiscuo".

1.21.3 L'utilizzo del proprio cellulare personale durante l'orario di lavoro è consentito laddove ricorrano ragioni di necessità e/o urgenza. L'utilizzo deve essere comunque improntato a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate

1.22 Il lavoro agile (o smart working) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli spaziali, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività. La definizione di smart working, contenuta nella Legge n. 81/2017 e ss.mm.ii., pone l'accento sulla flessibilità organizzativa, sulla volontarietà delle parti e sull'utilizzo di strumentazioni che consentano di lavorare da remoto.

1.22.1 Il dipendente che sia stato autorizzato allo svolgimento di attività lavorativa in regime di smart working verrà dotato - in via temporanea, se non già precedentemente assegnata - della strumentazione necessaria. Tale strumentazione può consistere in: pc fisso, pc portatile e/o telefono cellulare.

1.22.2 Il dipendente dovrà avere a casa, obbligatoriamente, una connessione internet disponibile, sia essa "fissa" (rame o fibra) oppure "mobile" (LTE/4G/5G). L'Ente non dovrà farsi carico di provvedere all'attivazione della connessione internet del dipendente.

1.22.3 Prima dell'attivazione dello Smart Working il dipendente dovrà farsi carico di ritirare la strumentazione presso il Servizio ICT il giorno precedente della data di attivazione e riconsegnarla non appena si termina la modalità smart; la consegna e la riconsegna verranno certificate da un apposito verbale. Tutte le attività di spostamento, trasporto e reinstallazione della strumentazione sono a carico del dipendente, con i rischi che ne derivano. Eventuali impossibilità o variazioni dovranno essere tempestivamente comunicate e concordate con il Servizio ICT.

1.22.4 La strumentazione consegnata permetterà al dipendente di accedere all'infrastruttura informatica dell'Ente, previa la connessione dell'utente in VPN con le credenziali fornite.

1.22.5 Qualora il dipendente debba attivare il trasferimento di chiamata dal telefono dell'ufficio verso il cellulare assegnatogli, oppure su uno che il dipendente stesso mette a disposizione, egli dovrà, previa formazione, attivare tale funzionalità sul proprio telefono fisso dell'ufficio il giorno precedente a quello previsto per lo Smart Working e disattivarla il giorno di rientro. Le chiamate in entrata pervenute al centralino e destinate all'operatore in Smart Working saranno trasferite al cellulare, proprio o a quello in dotazione. Il cellulare utilizzato per il trasferimento di chiamata, dovrà essere messo in protezione con l'inserimenti di un PIN di sicurezza.

1.22.6 In conformità al Regolamento UE 679/2016 in materia di protezione dei dati personali, il dipendente che lavora in Smart Working dovrà prestare particolare cautela nella

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

conservazione dei dispositivi a lui assegnati. L'eventuale perdita o sottrazione di uno di detti dispositivi costituisce un incidente informatico, che potrebbe divenire un serio rischio per la conoscibilità a terzi non autorizzati dei dati personali in esso contenuti. Nel caso in cui si verifichi un "databreach" - quale violazione di sicurezza che comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati - il dipendente sarà tenuto a darne immediata comunicazione all'Ufficio Protezione Dati e all'AdS

1.22.7 Il dipendente non potrà mai lasciare incustodito il bene a lui assegnato proprio per evitare un'eventuale sottrazione o perdita dello stesso.

1.22.8 Nessun soggetto terzo, oltre al dipendente autorizzato allo Smart Working, potrà conoscere il contenuto dei documenti di lavoro siano essi in forma cartacea che elettronica: pertanto il dipendente nell'esercizio della sua attività di smart working dovrà prestare ogni cautela in modo che terzi o familiari o conviventi non possano venire a conoscenza di detti dati personali utilizzati o di informazioni aziendali nei luoghi ove si esercita lo Smart Working.

1.22.9 Con il Decreto Legge del 17 marzo 2020, n.18, all'art.87 comma 2, è stata introdotta una forma di espletamento dello smart working in cui l'utente utilizza i propri apparati personali, non forniti dall'Ente, per lo svolgimento dell'attività lavorativa; questa modalità viene comunemente chiamata "*BYOD* (*Bring Your Own Device*)". In questo caso, l'utente dovrà comunicare la propria disponibilità all'uso di questa modalità, applicare al proprio apparato le misure minime di sicurezza secondo i parametri indicati dal Servizio ICT (esempi: "utilizzo di password per l'accesso al proprio apparato, antivirus professionale installato ecc."), coordinarsi con il Servizio ICT per il controllo degli apparati (anche da remoto) e l'eventuale approvazione.

1.22.10 In caso di utilizzo di piattaforme di videoconferenza, sia gratuite che a pagamento, sempre autorizzate dal Servizio ICT, è fatto divieto assoluto di registrazione delle sessioni/sedute, ove sia prevista la modalità integrata o con qualsiasi altro mezzo tecnologico atto alla registrazione dello schermo. E' parimenti vietata la cattura dello schermo ("screenshot") e divulgazione delle schermate/foto.

1.22.11 Alla strumentazione fornita si applicano tutte le norme già previste ai punti precedenti ed ai punti 4 e 6 del presente regolamento. Vista l'impossibilità di applicazione dei punti 4.2, 4.3, 4.4, legate al filtraggio dei siti internet (White list e Black list), resta comunque vietato ogni uso difforme rispetto all'attività d'ufficio. Nel caso di dispositivo di proprietà, si dovrà evitare l'accesso a fonti (siti web, supporti esterni, etc) potenzialmente dannose riguardo alla sicurezza dei dati.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

2. DOCUMENTI INFORMATICI

2.1 I documenti di lavoro andranno salvati esclusivamente negli archivi messi a disposizione dal Titolare (cartelle condivise e/o software gestionali).

2.2 I documenti creati durante le attività lavorative sono di esclusiva proprietà del Titolare, quindi non andranno eliminati se non previa autorizzazione/richiesta.

2.3 La cartella Documenti viene sincronizzata sui server del Titolare ed è di accesso esclusivo dell'utente. In caso di assenza del dipendente, sarà possibile ai soli Amministratori di Sistema accedere al contenuto di quella cartella, previa richiesta scritta del Dirigente del Settore. In questo caso, l'utente verrà informato dell'avvenuto accesso. In ogni caso il dipendente potrà conservare nella cartella "Documenti" legata al suo utente di dominio, solo documenti e dati che non siano di ufficio, ma che riguardano esclusivamente dati relativi al rapporto lavorativo come dipendente dell'Ente (buste paghe, comunicazioni del Servizio Personale, etc.).

2.4 In caso di spostamento all'interno della struttura organizzativa, sarà cura del dipendente consegnare al proprio responsabile l'eventuale contenuto della cartella, se contiene informazioni non inerenti al nuovo incarico.

2.5 In ogni caso, non sono ammessi documenti di tipo personale, di qualsivoglia formato (foto, video, etc). Il Titolare non è responsabile della perdita/alterazione dei suddetti dati se conservati sui propri sistemi.

2.6 Non è consentito l'uso di "cloud", se non espressamente richiesti dagli organi di vertice ed autorizzati dall'Amministratore di Sistema, previa verifica di adeguatezza alla normativa vigente. Di default questi servizi vengono inseriti in "Black List" (vedi ARTICOLO 4).

3. DOCUMENTI ANALOGICI

In caso di trattamenti senza l'ausilio di strumenti tecnologici bisogna osservare le seguenti prescrizioni:

3.1 Il dipendente non dovrà lasciare incustoditi i documenti contenenti dati personali a lui affidati per l'esercizio della sua attività.

3.2 Evitare il deposito di questi documenti in luoghi di transito come corridoi o sale riunioni.

3.3 Se la persona designata al trattamento dei dati è costretta ad allontanarsi momentaneamente non deve mai lasciare incustoditi i documenti e gli atti contenenti dati personali e sensibili sulle scrivanie o in altro luogo liberamente accessibile a terzi non autorizzati.

3.4 L'incuria può essere causa di sottrazione di documenti contenenti dati personali o aziendali con conseguente possibile trattamento illecito; il dipendente è perciò tenuto a rispettare quanto di seguito indicato:

- al termine della sessione di lavoro ricollocare i documenti negli appositi cassetti e contenitori evitando di mantenerli a vista sulla postazione assegnata per tutta la durata dell'assenza;
- usare promemoria volanti solo per indicazioni generiche;
- distruggere i dati cartacei contenenti dati sensibili qualora non debbano essere più utilizzati (es. mediante un tritadocumenti);
- qualora, per la mansione assegnata, il dipendente tratti abitualmente atti o documenti contenenti dati sensibili dovrà custodirli in armadi chiusi a chiave all'interno di uffici dotati di idonee misure di sicurezza. L'accesso a tali documenti sarà monitorato e consentito solo a coloro che ne sono stati espressamente autorizzati dal loro responsabile;

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

- qualora, per la mansione assegnata, il dipendente tratti solo accidentalmente atti o documenti contenenti dati sensibili, detti dati dovranno essere dallo stesso controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e dovranno essere immediatamente restituiti al termine delle operazioni affidate.

3.5 È severamente vietato utilizzare documenti contenenti dati personali, particolari o giudiziari come carta da riciclo o carta per appunti. Anche al fine di riduzione dei costi, è pertanto opportuno che – in caso di stampa di documenti – i dipendenti utilizzino la modalità “fronte/retro”.

3.6 Nei casi in cui l’utente presti la propria attività lavorativa in modalità “smart working”, deve essere assicurata la completa distruzione di copie, bozze e ogni altro documento, utilizzato durante l’attività, contenente dati personali. Si richiama, inoltre, l’osservanza del punto 1.22.8 del presente disciplinare

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

4. NAVIGAZIONE IN INTERNET

4.1 La postazione collegata ad Internet costituisce uno strumento necessario allo svolgimento dell'attività lavorativa, di conseguenza è proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

4.2 Tutti i dipendenti cui è assegnata una postazione di lavoro possono utilizzare Internet limitatamente ad una lista di siti preventivamente individuati dall'Ente (white list) e previa identificazione dell'utente attraverso le proprie credenziali. La lista dei siti istituzionali fruibili (white list) sarà progressivamente implementata e completata ed il novero di tali siti sarà deciso dal Servizio ICT.

4.3 Al fine di prevenire rischi di utilizzo improprio della rete reputati non compatibili con l'attività lavorativa, il Titolare utilizza dei sistemi di filtri che impediscono l'accesso diretto a siti non in linea con le finalità del Titolare (black list); questa viene progressivamente implementata e completata.

4.4 L'utilizzo completo di Internet, non filtrato dalla black list, è autorizzato, con richiesta formale all'AdS, per ciascun utente dal responsabile di Settore.

4.5 Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta e delle informazioni che vi immette. È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo i casi espressamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure assegnate.

4.6 È vietata ogni forma di registrazione a siti o mailing list i cui contenuti non siano legati allo svolgimento delle attività lavorative assegnate.

4.7 È vietata la navigazione di siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell'utilizzatore, non è consentito inoltre visitare né tanto meno memorizzare documenti dal contenuto oltraggioso, discriminatorio che offendono il comune senso del pudore.

4.8 Qualora il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario darne immediatamente segnalazione al Servizio ICT.

4.9 Non inserire i propri dati di login cliccando direttamente sui link contenuti all'interno di un'email, ma digitare l'indirizzo del sito manualmente per essere certi di non incorrere in siti contraffatti (es. phishing).

4.10 Non cancellare la sottoscrizione ad una mailing list di cui non si è certi dell'iscrizione (potrebbe trattarsi di un raggiro da parte di uno spammer per ottenere conferme sulla validità dell'indirizzo email dell'utente).

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

5. GESTIONE DELLA POSTA ELETTRONICA, PEC E FIRMA DIGITALE

5.1 L'utilizzo della posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Titolare assegna una casella email di posta personale e/o di servizio.

5.2 La casella di posta messa a disposizione dall'Ente è uno strumento di lavoro che deve essere quindi utilizzato esclusivamente per esigenze connesse all'attività lavorativa, non sono ammessi utilizzi diversi o privati dell'indirizzo; conseguentemente i dipendenti ai quali è assegnata sono responsabili del corretto utilizzo della stessa.

5.3 Si evidenzia che, nel caso di trasmissione di dati particolari (art. 9 GDPR) e/o giudiziari (art. 10 GDPR), è opportuno fare ricorso alla crittografia dei documenti.

5.4 È assolutamente vietato:

a. l'utilizzo di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti alla propria attività svolta per il Titolare;
b. inoltrare catene telematiche (es. petizioni, giochi) e altre forme di email che non abbiano attinenza con l'attività svolta;
c. utilizzare tecniche di "mail spamming", invio massiccio di comunicazioni a liste di utenti non aziendali;
d. allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi eseguibili, macro, script ecc.).

5.5 L'Ente provvederà a mettere a disposizione di ciascun dipendente apposite funzionalità di sistema, che consentano di inviare automaticamente, in caso di assenza dal Servizio dell'utente, messaggi di risposta che avvisino il mittente dell'assenza del destinatario, indicandogli, altresì, le coordinate di un altro lavoratore autorizzato a leggere le comunicazioni durante l'assenza.

5.6 Dopo la cessazione del rapporto di lavoro, l'account sarà rimosso previa disattivazione. L'account verrà disattivato decorsi quindici giorni dalla cessazione del rapporto: tale periodo servirà ad informare i terzi e a fornire a questi ultimi degli indirizzi alternativi cui rivolgersi per restare in contatto con gli Uffici del Titolare competenti per gli specifici procedimenti/affari.

5.7 In casi di assenza improvvisa o prolungata del dipendente, su richiesta del Dirigente competente, l'Amministratore di Sistema potrà accedere al contenuto della casella di posta elettronica al solo fine di recuperare messaggi urgenti per l'attività dell'Ufficio. Di tale accesso viene data immediata notizia al dipendente, con l'invito a modificare la password del proprio account al primo accesso al sistema successivo alla comunicazione.

5.8 È vietato l'utilizzo di caselle di posta personali (es. tiscali, gmail, live, etc…) a meno che non siano state autorizzate dagli organi di vertice. L'accesso a tali caselle viene bloccato tramite elenco di siti non fruibili (black list) visto il propagarsi, tramite tali caselle, di virus, malware e ramsonware.

5.9 È fatto obbligo al dipendente di controllare la cartella "spam" della propria casella di posta elettronica ogni trenta giorni per verificare se il sistema ha erroneamente catalogato alcuni messaggi ricevuti come "indesiderati".

5.10 Nel caso di mittenti sospetti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

5.11 Nel caso di messaggi provenienti da mittenti conosciuti e/o che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

5.12 L'Ente si è dotato di Posta Elettronica Certificata a disposizione dei vari uffici, gestibili tramite l'applicativo del Protocollo Generale. L'utilizzo di altre PEC non istituzionali non è consentito.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

5.13 L'Ente mette a disposizione dei dipendenti autorizzati la Firma Digitale. Questa viene rilasciata dal Funzionario del Servizio ICT, previa autorizzazione degli organi di vertice e presentazione di Documento di identità valido. Viene consegnata su smart card, per la cui lettura viene consegnato un lettore specifico. Oltre alla conservazione e alla cura, si richiede particolare attenzione a non conservare assieme alla smart card le credenziali di accesso (PIN e PUK). In caso di smarrimento/perdita di possesso, l'utente, dopo aver informato prontamente l'Amministratore di Sistema, effettuerà denuncia formale alle autorità competenti, inviandone copia. Si rammenta che la Firma Digitale è strettamente personale e l'uso da parte di terzi non è consentito, né altresì l'utilizzo al di fuori delle attività strettamente lavorative. È fatto obbligo di custodire adeguatamente i dispositivi di firma digitale, in modo che siano unicamente nella disponibilità dei soggetti a cui sono stati assegnati.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

6. MONITORAGGIO E TRACCIABILITA'

6.1 Il Titolare può avvalersi di sistemi di controllo per il corretto utilizzo degli strumenti di lavoro (che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di Dati personali riferiti o riferibili ai lavoratori) esclusivamente nel rispetto di quanto previsto dalle norme vigenti e dai provvedimenti delle competenti Autorità.

6.2 In particolare, il Titolare, nell'effettuare controlli sull'uso degli strumenti elettronici, eviterà un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

6.3 Le comunicazioni effettuate attraverso posta elettronica sono riservate, conseguentemente il contenuto non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Titolare o da parte di altri soggetti.

6.4 Le attività sull'uso di Internet vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema. Il trattamento dei dati contenuti nei LOG, può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

6.5 I dati personali contenuti nei LOG possono essere trattati esclusivamente in via eccezionale nelle ipotesi di seguito elencate:

a. rispondere ad eventuali richieste della polizia e/o dell'autorità giudiziaria;
b. richiesta dell'Amministratore di Sistema, limitatamente al caso di utilizzo anomalo degli strumenti informatici da parte degli utenti di una specifica Area/Settore (rilevabile esclusivamente dai dati aggregati) reiterato nel tempo.

6.6 I dati contenuti nei LOG sono mantenuti per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 180 (cento ottanta) giorni, e sono periodicamente cancellati automaticamente dal sistema.

6.7 I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301

GLOSSARIO

AdS: Amministratore di Sistema: Provv. Gen, 27/11/2008 (GU n.300 24/12/2008 e mod. 25/6/2009).
Bring your own device (BYOD) - chiamato anche **bring your own technology (BYOT), bring your own phone (BYOP), e bring your own PC (BYOPC)** - in italiano: porta il tuo dispositivo, porta la tua tecnologia, porta il tuo telefono e porta il tuo pc - è un'espressione usata per riferirsi alle politiche aziendali che permettono di portare i propri dispositivi personali nel posto di lavoro, e usarli per avere gli accessi privilegiati alle informazioni aziendali e alle loro applicazioni.
Black List: elenco di siti internet non accessibili da parte degli utenti della rete locale.
Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
DPO: Data Protection Officer o Responsabile Protezione dei Dati, art.37-38-39, Reg. UE 2016/679 (GDPR).
Log: archivio dei tracciati sulle attività di consultazione in rete locale e non.
Incaricati del trattamento dei Dati: non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4, par. 10, Reg. UE 2016/679 (GDPR), definizione di «terzo»).
Internet Service Provider: azienda che fornisce il servizio Internet (esempio telecom, tiscali, vodafone).
Postazione di Lavoro: personal computer collegato alla rete locale tramite la quale l'utente accede ai Servizi ed ai Dati da gestire.
Responsabile del trattamento dei Dati: secondo quanto elencato nell'art. 4, par. 8, Reg. UE 2016/679 (GDPR), per responsabile del trattamento si intende "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
Screenshot: fermo-immagine, schermata, immagine dello schermo o cattura dello schermo, indica ciò che viene visualizzato in un determinato istante sullo schermo di un monitor, di un televisore o di un qualunque dispositivo video.
Sistemi Portatili: notebook, smartphones e tablet.
Titolare del trattamento: secondo quanto previsto dall'art.4, par. 7, Reg. UE 2016/679 (GDPR) "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Utente e-mail (posta elettronica): persona autorizzata ad accedere al servizio di posta elettronica attraverso l'utilizzo di caselle e-mail.
Utente Internet: persona autorizzata ad accedere al servizio di navigazione in Internet.
Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
White List: elenco di siti internet accessibili da parte degli utenti della rete locale.

Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220 - Fax 0789/52301