Disciplinare d’uso delle risorse informatiche e dell’accesso ai servizi di rete

(Provvedimento del)

Indice

ART. 1 - RIFERIMENTI NORMATIVI

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE Regolamento generale sulla protezione dei dati)";
- Decreto Legislativo 10 agosto 2018 n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679" che ha modificato il Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";
- Deliberazione 1 marzo 2007 n. 13 del Garante della Privacy "*Linee guida del garante per posta elettronica e internet*" pubblicata sulla Gazzetta Ufficiale del 10 marzo 2007 n. 58;
- Direttiva 26 maggio 2009 n. 2 del Dipartimento della Funzione Pubblica "*Utilizzo di internet e della posta elettronica istituzionale sul luogo di lavoro*";
- Decreto Legislativo 7 marzo 2005 n. 82 "*Codice dell'Amministrazione Digitale*";
- Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n.2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto2015)".

ART. 2 – CAMPO DI APPLICAZIONE

Il presente Disciplinare si applica a tutti i dipendenti dell'Azienda Regionale per il Diritto allo Studio Universitario (di seguito "Azienda"), senza distinzione di categoria giuridica nonché a tutti gli eventuali prestatori d'opera o collaboratori dell'Azienda indipendentemente dal rapporto contrattuale con la stessa intrattenuto (studenti 150 ore, tirocinanti, stagisti, collaboratori coordinati e continuativi, etc…).

Il Disciplinare è pubblicato sull'Albo on line dell'Azienda e inserito nella sezione internet riservata al Personale, accessibile a ciascun Dipendente.

ART. 3 – FINALITA'

Il presente Disciplinare intende:

a) adottare indirizzi trasparenti, capaci di comunicare con chiarezza ai Colleghi le modalità di utilizzo degli strumenti informatici assegnati per lo svolgimento delle mansioni loro attribuite;

b) descrivere il diritto dell'Azienda a verificare l'uso corretto dei suddetti strumenti nonché le modalità con le quali l'Azienda esercita tale diritto di verifica.

Conformemente al Regolamento (Ue) 2016/679 (GDPR) di seguito vengono esposte le regole comportamentali da seguire per prevenire condotte che anche inconsapevolmente possano comportare rischi alla sicurezza dell'infrastruttura informatica dell'Azienda.

Per quanto non espressamente previsto dal presente disciplinare, si rinvia alle disposizioni generali vigenti in materia.

ART. 4 – APPARECCHIATURE INFORMATICHE IN DOTAZIONE AGLI UTENTI

Le pubbliche amministrazioni sono tenute ad assicurare il corretto impiego degli strumenti ICT e della telefonia da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa. Questo avviene nell'ottica di garantire la sicurezza, la disponibilità e l'integrità dei sistemi e di prevenire sprechi.
Viene quindi posto l'obbligo, in carico ai responsabili dei diversi Servizi nonché ai Dirigenti delle diverse Aree funzionali, di vigilanza sugli operatori delle proprie strutture al fine di verificare il corretto utilizzo degli strumenti di lavoro.

Il Personal Computer e le relative periferiche affidate all'utente sono strumenti di lavoro.

Eventuali utilizzi estranei all'attività lavorativa non sono consentiti in quanto possono contribuire a creare disservizi con conseguente necessità di sostenere costi straordinari di manutenzione e possono comportare rischi alla sicurezza dei dati e della rete dell'Azienda.

Il Personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento. Il Personal computer dato in affidamento all'utente permette l'accesso alla rete aziendale come meglio descritto nei successivi articoli del presente Disciplinare.

ART. 5 – PERSONALE AUTORIZZATO A COMPIERE INTERVENTI PER LA SICUREZZA E FUNZIONALITA'

Sono autorizzati ad effettuare gli interventi di seguito descritti solo tutti i Dipendenti assegnati al Servizio **Sistemi Informatici (ICT)**.

Limitatamente alle postazioni di lavoro utenti e limitatamente alle attività strettamente legate alla configurazione/gestione degli applicativi aziendali, il personale del **Servizio Applicativi e Amministrazione Digitale** deputati alla gestione degli applicativi, indipendentemente dalla sede territoriale di appartenenza, è autorizzato ad accedere alla postazione di lavoro interessata per svolgere le attività di propria competenza.

ART. 6 – INTERVENTI PER LA SICUREZZA E LA FUNZIONALITA'

L'Azienda rende noto che il Personale di cui all'art.5 è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia dei dati e del sistema stesso nonché a fronteggiare ulteriori difficoltà tecniche ovvero esigenze manutentive (ad es. aggiornamento/sostituzione/evoluzione di programmi, manutenzione hardware).

Il Personale incaricato di cui all'art.5 ha la facoltà di collegarsi e visualizzare in remoto il desktop dell'utente attraverso un software di connessione remota in maniera del tutto trasparente per i Colleghi in conformità alle norme che vietano il controllo a distanza dei lavoratori nonché alle misure di sicurezza dell'infrastruttura informatica.

L'intervento viene effettuato esclusivamente su chiamata dell'utente o d'ufficio in caso di oggettiva necessità (e comunque solo dopo aver preventivamente avvertito l'utente interessato) a seguito della rilevazione tecnica di problemi nel sistema informatico.

Le aree di memorizzazione del proprio PC o quelle condivise in rete che sono messe a disposizione dall'Azienda per lo svolgimento dell'attività lavorativa, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Su queste unità, vengono svolte regolari attività di verifica da parte del Personale del Servizio Sistemi Informatici ICT il quale potrà, in qualunque momento, procedere alla rimozione di ogni file o cartella chiaramente non inerente l'attività lavorativa (immagini personali, messaggi di posta personale, musica, video, etc…).

La stessa facoltà, sempre ai fini di garantire la salvaguardia e la sicurezza del sistema informatico e per ulteriori motivi tecnici e manutentivi, si applica anche in caso di assenza prolungata o impedimento dell'utente. E' fondamentale che ogni dipendente provveda periodicamente a pulire la propria area condivisa cancellando i file obsoleti o inutili; in caso contrario detta attività verrà svolta d'ufficio dal personale del Servizio Sistemi Informatici ICT. Particolare attenzione, inoltre, deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento.

ART. 6 BIS - DIVIETO DI MEMORIZZAZIONE SULLE RISORSE LOCALI DI FILE CONTENENTI DATI PERSONALI

Per prevenire fenomeni di violazione dei dati personali (c.d. "data breach") a fine della giornata lavorativa i Colleghi sono tenuti a cancellare file contenenti dati personali di studenti, dipendenti ed altre persone fisiche, dalle risorse locali del computer, salvando – se necessario – gli stessi file sulle risorse condivise messe a disposizione dal Servizio Sistemi Informatici ICT come riportato al successivo articolo 7.

Si ricorda altresì di svuotare contestualmente anche il cestino e di fare attenzione al contenuto della cartella "Download" o di altra cartella ove vengano scaricati i file dal browser utilizzato, provvedendo a rimuovere documenti contenenti dati personali.

ART. 7 - GESTIONE STRUMENTI ELETTRONICI (PC FISSI E PORTATILI)

Ciascun dipendente è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo: personal computer, periferiche, lettori di smart card, cellulari e altri dispositivi mobili).

E' obbligatorio adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Quanto riportato nell'art. 6 bis del presente Disciplinare si applica anche al presente articolo.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario osservare le seguenti prescrizioni:

- non salvare documenti contenenti dati personali di studenti, dipendenti e altre persone fisiche sulle risorse locali (hard disk della postazione pc o del notebook o comunque di qualsiasi dispositivo aziendale) o su dispositivi di memorizzazione esterni (hard disk esterni, chiavette usb) o ancora su dvd/cd-rom. Il Servizio Sistemi Informatici ICT rende disponibile per ciascun servizio, apposita risorsa remota, nella quale andranno salvati tali file;
- non dare evidenza delle credenziali di accesso al proprio pc (compresa la password di bitlocker), a Storefront, alla webmail, agli applicativi (come ad esempio, scrivendo su post-it login+password) o a servizi on line;
- le credenziali di accesso sono strettamente personali e non vanno comunicate ad altri soggetti;
- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici devono tassativamente essere chiusi a chiave;
- in caso di assenza momentanea dalla propria postazione accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. A tal fine è necessario chiudere la sessione di lavoro sul PC attraverso la disconnessione (logout) oppure, in alternativa, attivare un salvaschermo (screen-saver) protetto dalle credenziali di autenticazione.
  Relativamente allo screen-saver occorre osservare le seguenti prescrizioni:

  - non deve mai essere disattivato;
  - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
  - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito.

- quando si esegue la stampa di un documento contenente dati personali, in particolare

su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare che soggetti non abilitati al trattamento ne prendano visione.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- prima della riconsegna, rimuovere eventuali file ivi elaborati;
- quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
- quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
- in caso di furto di un portatile o di altro dispositivo mobile in dotazione è necessario avvertire tempestivamente il responsabile del Servizio Sistemi Informatici ICT onde prevenire possibili intrusioni ai sistemi aziendali;
- in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

E' ammesso l'utilizzo del PC Personale per l'accesso ad internet tramite la rete DSU solo ed esclusivamente in caso di assenza di una postazione aziendale fermo restando l'obbligo di utilizzare un antivirus aggiornato e/o adeguati sistemi di protezione e comunque dietro preventiva autorizzazione del responsabile del Servizio Sistemi Informatici ICT e dichiarazione di responsabilità da parte del dipendente.

ART. 8 - GESTIONE CREDENZIALI DI ACCESSO

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela il dipendente da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
- è necessario per gestire correttamente gli accessi a risorse condivise.

Fermo restando che sistemi quali Storefront, la posta elettronica aziendale nonché le impostazioni stesse del dominio sono configurate affinchè vengano rispettati i criteri di cui sotto, è necessario in tutti gli altri casi, seguire le seguenti indicazioni.

Ciascun dipendente deve scegliere le password in base ai seguenti criteri:

- deve essere lunga almeno otto caratteri;
- non deve fare riferimento ad informazioni agevolmente riconducibili a se stessi o ai propri amici/conoscenti/familiari;
- deve contenere una combinazione di numeri, caratteri speciali, lettere maiuscole e minuscole;
- non deve essere uguale alle precedenti.

Per la corretta gestione della password è inoltre necessario che la stessa:

- venga cambiata almeno ogni 60 giorni
- venga modificata al primo utilizzo;
- venga memorizzata o comunque conservata in un luogo sicuro;
- non venga mai rivelata ad alcun soggetto;
- non venga mia salvata automaticamente, sfruttando la funzione offerta da alcuni browser o applicativi

ART. 9 - INSTALLAZIONE DI HARDWARE E SOFTWARE

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti esclusivamente dal personale del Servizio Sistemi Informatici ICT, fatto salvo quanto previsto dall'articolo 5. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

- non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
- non installare sistemi per connessione esterne (es : modem, wi-fi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Sistemi Informatici ICT;
- non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Sistemi Informatici ICT, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

ART. 10 - GESTIONE POSTA ELETTRONICA AZIENDALE

L'Azienda fornisce un servizio di posta elettronica, mettendo a disposizione indirizzi con estensione @dsu.toscana.it; gli indirizzi sono individuali e personali. In caso di particolari esigenze si possono creare degli indirizzi di servizio previa richiesta del responsabile servizio stesso e condivisi tra più lavoratori.

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'Azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- al fine di sfruttare razionalmente lo spazio disponibile per la memorizzazione, ogni utente è soggetto a limiti di utilizzazione, il sistema avvisa l'utente all'approssimarsi del raggiungimento della quota limite impostata. Quando la quota viene superata non è più possibile inviare o ricevere messaggi fino a quando non viene liberato spazio sufficiente;
- il titolare di indirizzo di posta elettronica ha il dovere di controllare periodicamente la propria casella elettronica, verificare l'arrivo di nuovi messaggio, cancellare i messaggi obsoleti o inutili, verificare lo spazio occupato, prestare attenzione ai messaggi di quota raggiunta, ripulire la casella di posta prima del raggiungimento della quota massima consentita;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati per i quali l'ordinamento giuridico nazionale ed europeo prevedano particolari tutele, si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato,
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

E’ fatto assoluto divieto di trasmettere attraverso la mail, elenchi di dati personali di studenti, dipendenti ed altre persone fisiche senza che gli stessi vengano precedentemente criptati e protetti da password. Quest’ultima dovrà essere comunicata al destinatario attraverso un mezzo diverso dalla mail aziendale.

L'accesso alla propria casella di posta elettronica personale avviene attraverso l’utilizzo di credenziali comunicate dal personale incaricato. Per quanto concerne le credenziali di accesso si rimanda al precedente art. 8.

In caso di cessazione del rapporto di lavoro, l’indirizzo di posta elettronica individuale dell’interessato viene disattivato immediatamente

ART. 11 - GESTIONE DEL SALVATAGGIO DEI DATI

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Sistemi Informatici ICT esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni dipendente deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei dati personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). Il dipendente deve verificare che i supporti informatici utilizzati per il backup (dischi magnetici esterni, CD, DVD oppure flash disks/chiavette) siano funzionali e non corrotti.

ART. 12 - SUPPORTI RIMOVIBILI

Non è consentito utilizzare penne usb, hard-disk esterni, cd/dvd per memorizzare dati personali.
Fa eccezione a quanto sopra, il salvataggio su supporto ottico delle immagini di videosorveglianza richieste dalle forze dell’ordine o dall’autorità dai soggetti appositamente incaricati.
Nel corso della vigenza del presente disciplinare, verrà disabilitata la possibilità di inserire penne usb o altri dispositivi di memorizzazione esterna.
Esigenze particolari dovranno essere rappresentate al Servizio Sistemi Informatici ICT e da essi autorizzati in maniera formale.

ART. 13 - PROTEZIONE DALLE MINACCE INFORMATICHE

Per prevenire eventuali malfunzionamenti (anche non risolvibili) causati dalla presenza o dall’azione di virus, malware ed altre minacce informatiche, su ogni dispositivo dell’Azienda è installato un software antivirus con aggiornamento automatico delle definizioni e dell’applicazione.

Nel caso 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 è necessario darne immediatamente segnalazione al Servizio Sistemi Informatici ICT.

Si raccomanda di non scaricare e tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

ART. 14 - STAMPANTI E MATERIALI DI CONSUMO

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner) è riservato esclusivamente allo svolgimento di compiti di natura strettamente istituzionale.

Si consiglia, qualora la stampa cartacea non sia effettivamente necessaria, di produrre stampe in pdf attraverso la stampante virtuale installata ovvero di utilizzare, ove presente, la funzionalità di stampa fronte-retro o multipagina.

Il Personale incaricato può, laddove la stampante preveda questa funzionalità, monitorare il numero di stampe provenienti dai singoli pc e la quantità d'inchiostro consumata.

Nel corso della vigenza del presente disciplinare, ciascuna stampante/fotocopiatrice, verrà dotata di un PIN di accesso senza il quale non sarà possibile effettuare stampe o fotocopie.

ART. 15 - ACCESSO A INTERNET E COLLEGAMENTO ALLA RETE AZIENDALE

La navigazione in Internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione professionali; l'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro e al raggiungimento delle finalità istituzionali dell'Azienda.

L'accesso ad Internet è consentito a tutti i dipendenti dell'Azienda senza distinzione di categoria giuridica e senza limitazione alcuna ad eccezione:

- dei siti con contenuti a carattere pornografico, che inneggino a comportamenti violenti o discriminatori per genere, lingua, religione, razza, preferenze sessuali;
- dei siti per l'accesso a chat e riproduzione video;
- dei portali di accesso alle scommesse e al gioco d'azzardo.
- ogni altro sito ritenuto pericoloso o non idoneo al raggiungimento delle finalità istituzionali dell'Azienda

Al fine di prevenire il rischio di utilizzi impropri della rete, l'Azienda potrà, nel tempo, utilizzare e modificare il sistema di filtri che impediscano l'accesso diretto a siti che non hanno natura istituzionale. Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

Tutti gli utenti cui è assegnata una postazione di lavoro possono utilizzare Internet, compatibilmente con la banda a disposizione.

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

L'utente si impegna ad utilizzare Internet con la massima diligenza.

Non è consentito l'uso di programmi *peer to peer* per lo scambio di file in ambito privato

Non è consentito scaricare e/o scambiare materiale protetto da diritti di proprietà intellettuale senza averne titolo e comunque sempre e solo per attività connesse alle esigenze lavorative;

Non è consentito partecipare, a meno di esigenze professionali, a siti di chat, forum e/o social network.

ART. 16 - PROFILAZIONE DELL'UTENTE E MODIFICHE ORGANIZZATIVE

Le abilitazioni di accesso a specifici applicativi sono determinate dalle funzioni attribuite e dal ruolo esercitato da ogni dipendente; a fronte di modifiche delle funzioni o delle responsabilità svolte, il dipendente viene informato con messaggio di posta elettronica dei differenti livelli di accesso e di uso degli specifici applicativi, configurati dal Personale incaricato nei 30 (trenta) giorni successivi alle intervenute modifiche organizzative.

ART. 17– PASSWORD DI ACCESSO

Per quanto riguarda i criteri di sicurezza relativi alle password di accesso alle postazioni di lavoro ed ai programmi, trovano applicazione le disposizioni in materia di protezione dei dati.

La password di amministratore del dominio è conosciuta esclusivamente dagli operatori dei Servizio Sistemi Informatici ICT i quali sono tenuti a non divulgarla ad altri operatori interni o esterni.

La password di amministratore del pc è conosciuta solo dagli operatori del Servizio Sistemi Informatici ICT ed è fornita al personale del Servizio Applicativi e Amministrazione Digitale al fine di permettere l'installazione di applicativi/plugin o per attività di configurazione software di competenza. Analogamente a quanto previsto per la password di amministratore del dominio, anche quest'ultima non dev'essere divulgata ad altri operatori interni o esterni.

ART. 18 - TUTELA DELLA RISERVATEZZA DEI LAVORATORI. TRATTAMENTO DEI DATI E CONTROLLI.

Ai sensi della normativa vigente, al Datore di lavoro è preclusa la ricostruzione dell'attività del Lavoratore, anche tramite apparecchiatura software attraverso la lettura e registrazione dei messaggi di posta elettronica del lavoratore, la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore (usando la cache dei proxy), la lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo, l'analisi occulta di dispositivi portatili affidati dall'Azienda.

I trattamenti sui dati rispettano le garanzie in materia di privacy e si svolgono nell'osservanza dei seguenti principi:

- ✓ **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
- ✓ **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori;
- ✓ i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime, osservando **il principio di pertinenza e non eccedenza**. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
- ✓ le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del **principio di segretezza della corrispondenza**".

Nell'effettuare controlli sull'uso degli strumenti elettronici, l'Azienda evita un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'Azienda può adottare eventuali misure che consentano la verifica di comportamenti anomali attraverso un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a Dipendenti afferenti all'area o al servizio in cui è stata rilevata l'anomalia. In assenza di successive anomalie l'Azienda non effettua controlli su base individuale.

E' comunque esclusa, ai sensi della normativa vigente, l'attività di controllo prolungata, costante o indiscriminata.

Resta salva la collaborazione tecnica e la cooperazione applicativa con l'Autorità giudiziaria, in caso di attività di indagine o di esecuzione di misure cautelari, in conformità alle disposizioni di legge penale e civile.

ART. 19 - CONSERVAZIONE DEI DATI

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovrascrittura come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nei provvedimenti adottati dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Sulle postazioni su cui è installato il programma CCLEANER l'utente potrà agevolmente cancellare la cronologia dei siti visitati, i file temporanei e i cookies. In alternativa può utilizzare le medesime funzionalità previste dal proprio browser.

ART. 20 SANZIONI

L'inosservanza delle norme comportamentali descritte nel presente documento può comportare l'applicazione di sanzioni disciplinari ovvero di altre misure di tutela dell'Ente che si rendessero necessarie, incluso il risarcimento di eventuali danni arrecati alle apparecchiature, al software ed alle configurazioni in uso.

ART. 21 – ENTRATA IN VIGORE

Il presente Disciplinare entra in vigore dalla data di adozione del Provvedimento del Direttore e sostituisce completamente la precedente versione.

E' assicurata la massima diffusione del presente regolamento anche attraverso la pubblicazione nella Intranet Aziendale. Successivamente all'approvazione viene inviato a tutti i Colleghi unitamente al relativo Provvedimento di approvazione.