IRPET Istituto Regionale Programmazione Economica della Toscana

# DISCIPLINARE SICUREZZA INFORMATICA -USO DI INTERNET -GESTIONE POSTA ELETTRONICA E ALTRI STRUMENTI INFORMATICI

***(adottato con determinazione del Direttore n. 51 del 22.12.2020)***

**Indice generale**

## 1. INTRODUZIONE

L'Ente mette a disposizione del proprio personale e di eventuali collaboratori esterni i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- strumenti di informatica individuale, quali personal computer e relativi accessori, scanner ecc.
- apparati e servizi condivisi, quali ad esempio, posta elettronica, internet, stampanti di rete sistemi di condivisione file, server ecc.
- programmi di produttività individuale e procedure gestionali
- Applicativi specialistici per elaborazioni statistiche, programmazione e gestione banche dati.

Tali risorse costituiscono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.
Il documento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'Ente nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei propri sistemi informativi.
In particolare si evidenzia come l'utilizzo delle risorse informatiche per scopi non inerenti all'attività lavorativa possa contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle infrastrutture dell'Ente.
Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare, dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e dai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali. Tra questi rientrano le "Linee guida del Garante per posta elettronica e internet" emesse in data 1 marzo 2007. L'Ente non effettua registrazioni per il controllo dell'attività lavorativa dei dipendenti, ma solo registrazioni volte a salvaguardare la sicurezza ed il mantenimento dell'efficienza dei sistemi. I dati registrati automaticamente a tale scopo non vengono utilizzati in alcun modo per il controllo a distanza dei lavoratori e le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.

## 2. CAMPO DI APPLICAZIONE

Le regole descritte nel presente documento devono essere rispettate da tutto il personale dell'Ente (inclusi i consulenti esterni), indipendentemente dal tipo di incarico svolto e dalla sede dell'attività.
La gestione delle risorse strumentali, ivi incluse quelle informatiche, compete ai Dirigenti, che si assumono le responsabilità legate al corretto utilizzo ed all'osservanza delle norme.

## 3. NORMATIVA DI RIFERIMENTO

Il presente Disciplinare Interno è redatto in conformità alla normativa alla normativa vigente, di seguito riportata per riferimento:

- Normativa in materia di diritto d'autore e di altri diritti connessi al suo esercizio introdotta con la Legge n.633/41 per la protezione delle opere dell'ingegno di carattere creativo qualunque ne sia il modo o la forma di espressione.
- Normativa in materia di protezione del software introdotta con il D.Lgs. n.518/92 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori"; tale provvedimento normativo ha infatti aggiunto l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori, all'art.171 della Legge n° 633/1941. L'art. 171-bis, il cui testo è stato ultimamente modificato dalla L. n° 248/2000 "Nuove norme di tutela del diritto d'autore", prevede sanzioni penali a carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di copyright; pertanto la norma pone il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie.

- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori).
- Costituzione della Repubblica Italiana, art. 15 sancisce che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge".
- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza – "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.
- Regolamento 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 30 giugno 2003, n°. 196 "Codice in materia di protezione dei dati personali" e s.m.i., (da ultimo modificato dal D.LGS. 101/2018) garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali e della dignità dei soggetti a cui si riferiscono i dati, imponendo l'adozione di misure di sicurezza che riducano il rischio informatico e consentano un efficace controllo sull'utilizzo e la conservazione dei dati. Il decreto prevede un livello minimo di sicurezza per i dati personali definendo le misure fisiche, logiche e organizzative che devono essere adottate al fine di: evitare possibili distruzioni, perdite, alterazioni di dati; garantire che l'accesso ai dati sia effettuato dalle sole persone incaricate al trattamento e quindi autorizzate; garantire che il trattamento avvenga per le finalità e nelle modalità consentite.
- 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° agosto 2015)" Le misure di sicurezza sono applicate garantendo il rispetto di quanto disposto dalle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007.
- Raccomandazioni del Cert-PA di AgID per la sicurezza dello smart working 17 marzo 2020.
- Codice di comportamento dei dipendenti pubblici (DPR 62/2013) e Codice di comportamento dei dipendenti di IRPET approvato con "determinazione del Direttore n.42 del 30.09.2019"

# 4. UTILIZZO DELLE POSTAZIONI DI LAVORO

## 4.1. Principi generali

In funzione del proprio ruolo e delle esigenze organizzative e lavorative, il personale in servizio presso l'Ente è dotato di personal computer per lo svolgimento di attività connesse agli incarichi lavorativi, nel rispetto delle regole di seguito descritte.
Il personal computer affidato al dipendente è quindi uno strumento di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione dall'Ente.
Le pubbliche amministrazioni sono tenute ad assicurare il corretto impiego degli strumenti ICT e della telefonia da parte dei propri operatori, 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. Esiste quindi in capo agli operatori l'obbligo, sancito da norme di legge e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa, e questo anche nell'utilizzo delle risorse aziendali. In particolare l'art. 11 comma 3 del Codice di comportamento dei dipendenti dell'Ente prevede che "*Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione.*". Tale prescrizione riguarda quindi anche l'uso delle risorse informatiche, nell'utilizzo delle quali il dipendente deve agire in modo da non pregiudicare e ostacolare le attività dell'Ente o perseguire interessi privati in contrasto con quelli pubblici.
La Corte dei Conti ha spesso sanzionato l'indebito utilizzo della connessione Internet e della posta elettronica da parte di un dipendente, statuendo che esso configuri profili di responsabilità a carico del medesimo per il danno patrimoniale cagionato all'Amministrazione, consistente nel mancato svolgimento della prestazione lavorativa. A tal proposito la Corte ha inoltre osservato che, a seguito di ripetute e significative anomalie (ad esempio presenza di virus provenienti da siti non istituzionali), l'Amministrazione possa svolgere verifiche ex post sui dati inerenti l'accesso alla rete dei propri operatori.
Viene quindi posto l'obbligo, in carico ai dirigenti, di vigilanza sugli operatori delle proprie strutture al fine di verificare l'effettivo adempimento della prestazione lavorativa e il corretto utilizzo degli strumenti di lavoro. Ogni abuso in tal senso dovrà essere prontamente rilevato ed eventualmente sanzionato.

## 4.2. Regole di utilizzo

Le postazioni di lavoro, normalmente, sono connesse alla rete interna dell'Ente con lo scopo di usufruire dei servizi dell'Ente, accedere alle applicazioni software gestite centralmente dal servizio informatico, condividere informazioni, fruire i contenuti dell'Intranet.

Per una corretta gestione delle postazioni di lavoro è necessario osservare alcune **regole**:

- Le informazioni archiviate nella postazione devono essere esclusivamente quelle inerenti la propria attività lavorativa;
- Il salvataggio (backup) dei dati necessari all'attività lavorativa, per le postazioni che non memorizzano i propri dati sul file server centrale (server cloud), è di esclusiva responsabilità dell'utente, fermi restando i vincoli derivanti dalle disposizioni del GDPR 679/2016;
- La modifica dei componenti interni (aggiunta, rimozione, sostituzione) delle attrezzature informatiche messe a disposizione è di esclusiva competenza del personale del Servizio Informatico;
- La modifica delle configurazioni software impostate sulla propria o altrui postazione di lavoro, è consentita esclusivamente al personale del Servizio Informatico: l'utente può eventualmente procedere ad eventuali modifiche solo dopo aver avuto esplicita autorizzazione a farlo.
- L'attivazione o la modifica di password di sistema (ad es. quelle a protezione del BIOS del computer), è consentita solo a seguito di esplicita autorizzazione del personale del Servizio Informatico.

- Non è consentita l'installazione di programmi applicativi diversi da quelli predisposti e/o autorizzati dal Servizio Informatico inclusi, tra gli altri, browser per la navigazione internet e software di office automation. Le richieste di installazione e aggiornamento di ulteriori applicativi rispetto a quelli autorizzati devono essere preventivamente validate dal Servizio Informatico in ordine alle necessarie verifiche tecniche. Qualora venissero riscontrati programmi non autorizzati sulle postazioni di lavoro, anche se legali, questi verranno disinstallati dal personale tecnico addetto alla manutenzione delle postazioni di lavoro.
- E' vietato l'utilizzo tramite collegamento alla rete locale dell'Ente, di dispositivi informatici personali non forniti dall'Ente (quali ad esempio pc, notebook, tablet, smartphone, periferiche etc.), salva preventiva ed espressa autorizzazione del dirigente responsabile del Servizio Informatico. Tali dispositivi, propri del personale dipendente come di collaboratori/soggetti visitatori, potranno essere collegati esclusivamente alla rete wifi appositamente messa a disposizione degli ospiti. In caso di espressa autorizzazione dirigenziale all'uso della rete locale, l'utente è tenuto a rispettare le configurazioni di sistema disposte dal Servizio Informatico ed il rispetto delle misure minime di sicurezza descritte nell'allegato B del D.Lgs 196/2003 e ssmm.
- La riproduzione o la duplicazione di programmi, può essere effettuata solo nel pieno rispetto della vigente normativa in materia di protezione della proprietà intellettuale.
- Si sconsiglia l'uso di dischetti, CD-ROM o analoghi supporti di memorizzazione di incerta provenienza che potrebbero causare danni alla postazione di lavoro; L'uso di memorie USB, data l'estrema facilità con cui possono prestarsi alla diffusione di virus e malware, è da evitare.
- È proibito duplicare documenti contenenti dati personali particolari e sanitari su supporti removibili o su sistemi di rete non gestiti dal personale del Servizio Informatico (ad es. su cloud o qualsiasi servizio col quale l'Ente non abbia stipulato apposita convenzione e Accordo di Protezione Dati (DPA), come per esempio i vari servizi dropbox, onedrive, slack, ecc.).
- È vietata l'installazione non autorizzata dal Servizio Informatico di propri dispositivi di connessione come Access Point, Router, Printer server, modem etc alla rete dell'Ente.
- In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, informare tempestivamente il Servizio Informatico comunicando quali dati erano contenuti all'interno.
- Effettuare sempre il log-out dai servizi/portali utilizzati una volta conclusa la sessione lavorativa evitando la semplice chiusura della finestra del browser.
- Al termine del lavoro deve essere correttamente chiusa la sessione e devono essere spenti computer, video ed accessori.
- L'accesso al sistema deve essere bloccato e/o deve essere impostata la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro anche per bervi intervalli di tempo.
- Costituisce buona prassi effettuare con cadenza periodica (almeno ogni sei mesi) la pulizia degli archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati.
- La tutela della gestione locale dei dati presenti sulle stazioni di lavoro personali (personal computer) è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, salvataggi su supporti di rete (cloud o altre condivisioni dedicate allo scopo).
- Nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali.

Il personale che svolge attività lavorativa da luoghi diversi dalla sede, in modalità **smart working** o **telelavoro** è tenuto a seguire le seguenti ulteriori disposizioni:

- Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette, ovvero l'accesso alla rete wifi di casa o in generale del luogo dove è collocata la postazione deve richiedere un'autenticazione con livello di sicurezza almeno WPA2 con una chiave di lunghezza e complessità adeguata (lo standard attuale è di 24 simboli).
- Collegare solo dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione).
- Il dipendente in smart working è tenuto a custodire con diligenza la documentazione, i dati e le informazioni dell'Amministrazione utilizzati in connessione con la prestazione lavorativa;
- Il dipendente è tenuto comunque anche in telelavoro al rispetto delle previsioni del Regolamento UE 679/2016 e del D.Lgs. n. 196/2003 in materia di privacy e protezione dei dati personali.
- In ottemperanza alle disposizioni comunitarie e nazionali nonché di contratto, il dipendente è tenuto alla più assoluta riservatezza sui dati e sulle informazioni in suo possesso e/o disponibili sul sistema informativo e conseguentemente dovrà adottare – in relazione alla particolare modalità della Sua prestazione – ogni provvedimento idoneo a garantire tale riservatezza.
- Inoltre, nella qualità di "autorizzato" del trattamento dei dati personali, anche presso il proprio luogo di prestazione fuori sede, dovrà osservare tutte le istruzioni e misure di sicurezza previste.

In particolare, con riferimento alle modalità smart working, il dipendente dovrà:

- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione fuori sede;
- procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- qualora non si utilizzino dispositivi forniti dal titolare del trattamento si proceda ad installare almeno un buon sistema antivirus ed effettuare un'accurata scansione preventiva;
- evitare l'uso sulla postazione e i dispositivi di lavoro dei social network, o altre applicazioni social facilmente hackerabili;
- adoperare "misure di sicurezza" nell'utilizzo di pc o tablet come paraschermi (privacy-screen) che impediscano la visuale laterale del vicino, non tanto e solo per motivi di riservatezza, ma anche per la circolazione dei dati;
- evitare di rivelare al telefono informazioni di carattere personale;
- evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie;
- alla conclusione della prestazione lavorativa giornaliera conservare e tutelare i documenti eventualmente stampati provvedendo alla loro eventuale distruzione solo una volta rientrato presso la Sua abituale sede di lavoro;
- qualora, invece, al termine del lavoro risulti necessario trattenere presso il proprio domicilio materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura e, dunque, debitamente chiusi.

Nello specifico, quindi, il dipendente in regime di smart working è responsabile delle attrezzature che gli sono affidate in uso e pertanto deve provvedere a mantenerle in completa efficienza segnalando tempestivamente al Servizio Informatico ogni eventuale problema tecnico e, in caso di dubbio, sulla sicurezza della postazione di lavoro.
Le suddette norme comportamentali devono essere osservate anche nei casi eccezionali di utilizzo di risorse informatiche non fornite direttamente dal Servizio Informatico.
Ai soli fini di prestare assistenza tecnica informatica ai lavoratori, l'Ente utilizza alcuni software che permettono all'amministratore di sistema di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente di intervenire attivamente. L'attivazione di tale funzionalità può essere richiesta solamente da parte degli amministratori di sistema e solo quando strettamente necessario per poter svolgere l'attività di assistenza tecnica informatica e deve essere sottoposta ad un preventivo e contestuale consenso da parte del lavoratore.

## 5. CREDENZIALI E PASSWORD

### 5.1. Principi generali

Le credenziali (nome utente e password) per l'accesso ai servizi informatici dell'Ente vengono rilasciate dal Servizio Informatico previa richiesta; il personale del servizio provvede inoltre a rigenerare password scadute o dimenticate ed a disattivare le utenze cessate. L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi e alle risorse dell'Ente, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente gravissimi (ad es.visualizzazione di informazioni riservate, alterazione o distruzione di dati, uso improprio della propria posta elettronica etc.).

### 5.2. Regole di utilizzo

Per una corretta gestione delle credenziali di autenticazione è necessario osservare le seguenti regole:

- modificare alla prima connessione la password che il Servizio Informatico attribuisce e comunica;
- usare nella composizione della password almeno un carattere numerico, uno maiuscolo e uno speciale e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale:
- modificare la password almeno ogni 90 giorni e, nel caso di trattamento di dati personali particolari e/o giudiziari, almeno ogni 30 giorni secondo le disposizioni contenute nell'allegato B del D.Lgs 196/2003 e ssmm; nel caso in cui si ritenga che la propria password sia stata compromessa, modificarla immediatamente;
- mantenere la password riservata, non divulgarla a terzi: l'utente è responsabile penalmente e civilmente di abusi o incidenti di sicurezza nel caso in cui non custodisca adeguatamente le proprie credenziali;
- non trascriverla su supporti facilmente accessibili a terzi (ad es. foglietti, post-it etc.);
- non permettere ad altri utenti o colleghi di operare con le proprie credenziali;
- comunicare tempestivamente ai Sistemi Informativi trasferimenti e cessazioni, in modo da consentire la disabilitazione dell'accesso ai servizi non strettamente necessari;

Le password sono personali e riservate, si fa presente però che in caso di prolungata assenza o impedimento dell'utente, che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Dirigente dell'area o del servizio di appartenenza dell'utente, in qualità di fiduciario, può richiedere al Servizio Informatico che venga effettuato il reset della password dell'utente stesso. Al termine del tempo strettamente necessario al recupero delle informazioni di lavoro protette da password, il suddetto Responsabile dovrà richiedere al Servizio Informatico un nuovo reset della password che, questa volta, sarà comunicato esclusivamente all'utente interessato.

Altri dispositivi coinvolti in sistemi di autenticazione (per esempio certificati su smartcard o supporto USB, CNS) devono essere diligentemente tenuti sotto sorveglianza, mai lasciati incustoditi anche in occasione di brevi assenze e devono essere riposti in luoghi ad accesso controllato al termine della sessione lavorativa. Il loro utilizzo è strettamente personale e non delegabile.
Smartphone aziendali o personali utilizzati per accessi a servizi con sistemi di autenticazione a doppia chiave (OTP) devono avere attivati sistemi di autenticazione.

## 6. USO DELLA POSTA ELETTRONICA

### 6.1. Principi generali

L'Ente fornisce un servizio di posta elettronica, mettendo a disposizione indirizzi con dominio @irpet.it; gli indirizzi possono essere individuali o per servizio, questi ultimi vengono richiesti dal responsabile dello stesso e condivisi tra più lavoratori. Il servizio di posta elettronica è uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali. Il data base di posta è di esclusiva proprietà dell'Ente, il personale del Servizio Informatico

per motivi tecnici e di sicurezza, in particolare per prevenire o correggere malfunzionamenti, può accedere al suo contenuto nel rispetto della normativa vigente.

### 6.2. Regole di utilizzo

Per l'uso del servizio di posta elettronica, si richiede di osservare le seguenti norme comportamentali:

- la casella di posta elettronica nominale è riservata esclusivamente al personale assunto con contratto di lavoro subordinato a tempo determinato o indeterminato o titolare di specifica borsa di studio conferita dall'Ente. E' possibile la creazione di caselle di posta non nominali – utilizzabili anche da personale privo di contratto di lavoro subordinato a tempo determinato o indeterminato – finalizzate a specifici progetti, che devono essere chiuse al termine del progetto cui sono associate; sarà cura del dirigente responsabile del progetto richiedere al Servizio Informatico l'istituzione della casella e comunicare il termine per la sua chiusura;
- l'uso della posta elettronica aziendale è consentito esclusivamente per motivi attinenti allo svolgimento delle mansioni assegnate: l'utente del servizio è consapevole che i contenuti della posta elettronica dell'Ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa;
- collegarsi al server di posta (sia dall'interno che dall'esterno della rete dell'Ente) all'indirizzo https://smail.servizi.tix.it;
- il Servizio Informatico fornisce assistenza all'uso ed alla configurazione esclusivamente per i programmi client autorizzati su dispositivi di proprietà dell'Ente;
- 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; la responsabilità per la perdita di messaggi dovuta al raggiungimento del limite è in capo all'utente;
- limitare la dimensione dei messaggi inviati, soprattutto nel caso di destinatari multipli; un allegato di grandi dimensioni potrebbe impedire il corretto smistamento del messaggio o richiedere un uso eccessivo delle risorse;
- qualora sia necessario ricevere o spedire documenti di dimensioni maggiori del normale, è opportuno concordare con il Servizio Informatico le modalità di compressione dei dati, anche nell'interesse del soggetto destinatario;
- è richiesto, nei messaggi in uscita, riportare in calce la firma del soggetto mittente contenente, al minimo: nome, cognome ed Ufficio/Servizio di appartenenza, numero di telefono aziendale;
- è necessario porre particolare attenzione ad aprire allegati contenenti programmi "eseguibili" o comunque di dubbia natura o provenienza ed effettuare sempre un controllo antivirus preventivo su di essi;
- è illecito scambiare messaggi sotto falsa identità, ovvero impersonando un altro mittente;
- dato il carattere istituzionale delle caselle di posta dell'Ente è fatto divieto inoltrare all'esterno messaggi non inerenti le proprie competenze nell'Ente ed utilizzare l'indirizzo di posta globale (c.d. broadcast) per motivi non legati all'attività lavorativa ed istituzionale;
- poiché la posta elettronica diretta all'esterno della rete informatica dell'Ente può essere intercettata da estranei, l'invio tramite tale mezzo di documenti di lavoro "strettamente riservati" è sconsigliato e comunque va valutato con particolare attenzione;
- alla cessazione dell'attività lavorativa presso l'Ente, la casella di posta elettronica del dipendente sarà disattivata e successivamente eliminata, l'utente è pertanto invitato a salvare o inoltrare ad altri i messaggi che fossero necessari per le successive esigenze lavorative del servizio prima delle

dimissioni. Quindici giorni prima della cessazione del rapporto di lavoro, su indicazione del dirigente responsabile del titolare della casella e/o del Servizio Amministrazione, il Servizio Informatico provvederà a comunicare all'interessato la prossima chiusura della propria casella di posta – che deve avvenire l'ultimo giorno di servizio - , invitandolo al salvataggio di eventuali contenuti di interesse e fornendo assistenza nell'operazione, se richiesto.

# 7. USO DELLA RETE LOCALE, INTERNET E RISORSE CONDIVISE

## 7.1. Principi generali

Di norma ogni postazione di lavoro è connessa alla rete locale dell'Ente e agli utenti sono fornite le credenziali per l'accesso alla intranet, ad internet ed alle risorse di rete condivise funzionali all'attività lavorativa. Tali accessi devono avvenire esclusivamente per finalità istituzionali, strettamente connesse agli incarichi lavorativi svolti e sempre nel rispetto delle regole elencate in questo documento.

## 7.2. Regole di utilizzo

Per l'uso dei servizi connessi ad internet, alla rete locale ed alle risorse di rete condivise, valgono le seguenti norme comportamentali:

- non è consentito navigare in internet in siti non attinenti allo svolgimento delle mansioni assegnate;
- non trasferire sulla propria postazione di lavoro, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento del computer;
- non 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 l'uso di programmi peer to peer per lo scambio di file in ambito privato;
- non partecipare, a meno di esigenze professionali, a siti di chat, forum e/o social network;
- non pubblicare testi, immagini o video a contenuto blasfemo, osceno o diffamatorio;
- è vietata ogni forma di registrazione a nome dell'Ente o fornendo i dati relativi ad e-mail istituzionali a siti i cui contenuti non siano legati all'attività lavorativa;
- cercare di limitare, ogni volta che sia possibile, le stampe in modo da risparmiare preziose risorse e non intralciare il lavoro altrui;
- a ogni utente e a ogni ufficio che ne faccia richiesta, viene assegnato uno spazio sui file server centrali; le cartelle presenti nel server sono aree di salvataggio e/o condivisione di informazioni strettamente professionali: non possono in alcun modo essere utilizzate per scopi diversi;
- il materiale non pertinente all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, su personal computer o in sulle cartelle di rete condivise. Il personale del Servizio Informatico può procedere in ogni momento alla rimozione di materiale ritenuto non pertinente o potenzialmente pericoloso senza preavviso;
- sulle unità di rete condivise vengono svolte regolari attività di controllo, amministrazione e back up da parte del Servizio Informatico, in caso di perdita dei dati è possibile rivolgersi al Servizio Informatico per recuperare i dati mancanti;
- lo spazio disco messo a disposizione ha dei costi notevoli sia in termini economici che di tempo dedicato alla manutenzione, pertanto ogni utente periodicamente provvede alla cancellazione dei file obsoleti o inutili; Al superamento del limite individuale impostato per la quantità di informazioni, per validi e giustificati motivi, è possibile per il responsabile del servizio richiedere al Servizio Informatico un ampliamento dello spazio a disposizione.

# 8. CESSAZIONE DEL RAPPORTO DI LAVORO

Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'Ente tutte

le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per i Servizi.
La fase di cessazione prevede le seguenti modalità operative:

- le credenziali fornite all'utente verranno disabilitate: è cura del responsabile del Servizio interessato comunicare le cessazioni degli utenti al Servizio Informatico;
- la casella di posta elettronica individuale verrà disattivata e successivamente cancellata: le attività necessarie per il passaggio delle consegne e la copia del materiale di interesse dell'Ufficio dovranno essere effettuati prima della disattivazione, a cura del responsabile del Servizio interessato; l'utente avrà a disposizione due settimane, salvo diversi accordi col Servizio Informatico, per la copia e salvataggio del contenuto della casella di posta elettronica nelle due settimane precedenti la data di cessazione del rapporto. A partire dalla data di cessazione del rapporto di lavoro la casella sarà chiusa e successivamente cancellata ed il suo contenuto non potrà essere recuperato dall'utente, senza alcuna pretesa in merito.
- le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio e legate alla casella di posta elettronica del dipendente, dovranno essere portate a conoscenza del Dirigente in tempo utile per consentire una loro migrazione verso altri utenti, ovvero la loro disabilitazione.
- le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore dell'Ente restano nella piena ed esclusiva disponibilità dell'Ente. L'utente non può formare, ottenere copia e/o cancellare documenti ed informazioni di interesse dell'Ente presenti sulle postazioni di lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro a meno di esplicita autorizzazione scritta preventiva da parte del responsabile della struttura di appartenenza;
- le informazioni eventualmente lasciate sulle postazioni di lavoro o sulle risorse di rete che non siano di interesse per l'Ente verranno cancellate al termine del rapporto di lavoro senza alcuna responsabilità per l'Ente

# 9 . INTERVENTI DI ASSISTENZA E MANUTENZIONE

## 9.1. Principi generali

Il personale del Servizio Informatico ha tra i suoi compiti quello di garantire il funzionamento generale della infrastruttura (sicurezza informatica, backup, rete, server, progettazione informatica ecc.) e dedica le proprie risorse in via prioritaria allo svolgimento di tali attività; le richieste di assistenza ai singoli vengono gestite con le modalità indicate di seguito.

### 9.2. Regole di utilizzo

Per le richieste di assistenza, valgono le seguenti norme comportamentali:

- Le richieste vanno inoltrate attraverso messaggi di posta elettronica al Servizio Informatico, indicando chiaramente il tipo di inconveniente riscontrato ed ogni tipo di informazione utile a diagnosticare il problema, evitando indicazioni generiche come "non va", "non funziona", etc. Un messaggio di posta elettronica confermerà la presa in carico da parte del tecnico;
- Le richieste vengono evase in ordine di ricezione, dando priorità agli interventi che coinvolgono più utenti o che mettono a rischio la continuità dei servizi erogati al pubblico;
- Lo svolgimento di attività che richiedono impegni finanziari per essere svolte, è soggetto a valutazioni di convenienza economica da parte del Servizio Informatico ed alla verifica della copertura finanziaria necessaria;

# 10. PROCEDURE DI ACQUISTO E SOSTITUZIONE

Il materiale informatico (hardware e software) è soggetto a guasti e ad obsolescenza e le risorse a disposizione del Servizio Informatico e/o delle aree o servizi possono risultare inadeguate per soddisfare le nuove esigenze che dovessero manifestarsi nel tempo.

L' acquisto e la sostituzione di prodotti informatici (hardware e software) prevede le seguenti modalità operative:

- Ogni anno, entro il mese di novembre, i responsabili delle aree e dei servizi comunicano al direttore dell'Ufficio competente (attualmente il Servizio Informatico) le proprie necessità per l'anno successivo, al fine di permettere la redazione di un Piano Acquisti generale;
- In caso di richieste urgenti, ad esempio dovute a guasti o altri imprevisti, ogni utente si rapporta al proprio responsabile che – valutata l'effettiva necessità - provvede a compilare ed inoltrare richiesta al Servizio Informatico;
- Il personale del Servizio Informatico, valutata sul piano tecnico la congruità delle richieste pervenute e verificata l'adeguata copertura finanziaria, effettua in collaborazione col Servizio Amministrazione e l'Ufficio di Supporto Giuridico la procedura di acquisto.
- Gli acquisti e le modifiche alle procedure informatiche (gestionali etc.) devono essere inderogabilmente sottoposte al Servizio Informatico che provvederà all'analisi dei requisiti, alla valutazione del merito, al contatto con i fornitori ed al successivo supporto agli utenti.

## 11. SVILUPPO

Il Servizio Informatico provvede allo sviluppo dell'infrastruttura informatica dell'Ente e ne cura la successiva manutenzione.
La gestione di progetti congiunti con altri Servizi e Aree è strutturata in modo tale per cui le attività aventi ricadute, anche indirette, sui Sistemi Informativi dell'Ente debbano prevedere il coinvolgimento del Servizio Informatico a partire dalla fase di progetto fino alla conclusione dei lavori, in modo da ottimizzare l'integrazione con l'infrastruttura esistente sia hardware che software con particolare riferimento alle attività legate a reti, cablaggi, procedure informatiche da ospitare presso i Sistemi Informativi o da alimentare con dati di pertinenza dell'Ente evitando costose duplicazioni e pericolose incompatibilità;

## 12. CONTROLLI

L'Ente, utilizzando sistemi informativi per esigenze produttive o organizzative (ad esempio per rilevare anomalie o per manutenzione), può avvalersi nel rispetto dell'art. 4 comma 2 dello Statuto dei Lavoratori, di sistemi che permettano un controllo indiretto a distanza (controllo preterintenzionale) e determinano un trattamento di dati riferiti o riferibili ai lavoratori, nel rispetto delle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei dati personali il 1 marzo 2007;

L'Ente non effettua, in alcun caso, trattamenti di dati personali mediante sistemi informatici che mirino al controllo a distanza dei lavoratori, grazie ai quali sia possibile ricostruire la loro attività e che vengano svolti con i seguenti mezzi:

- ✓ Lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto tecnicamente necessario per fornire il servizio di posta stesso;
- ✓ memorizzazione ed eventuale riproduzione delle pagine web visitate dal dipendente;
- ✓ lettura e registrazione dei caratteri inseriti dai lavoratori mediante tastiera;
- ✓ analisi occulta di computer affidati in uso;

Le attività di controllo, legittimamente svolte dall'Ente ai sensi del presente disciplinare, si attengono in ogni caso ai seguenti principi fondamentali:

1. **Necessità, pertinenza e non eccedenza**: I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì il principio di pertinenza e non eccedenza. L'Ente raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti e sono mirate sull'area individuata come "di rischio".

2. **Finalità e correttezza**: I trattamenti sono effettuati per finalità determinate, esplicite e legittime. Le finalità perseguite dall'Ente riguardano o possono riguardare, caso per caso:

- sicurezza sul lavoro
- sicurezza dei sistemi e relativa risoluzione di problemi tecnici
- esigenze di organizzazione
- esigenze di produzione
- rispetto di obblighi legali
- tutela dell'Ente

3. Le attività che comportano l'uso del servizio di accesso ad internet verranno automaticamente registrate in forma elettronica da un apparato informatico (proxy) e memorizzate su log di sistema con le sole finalità statistiche sull'utilizzo dell'infrastruttura;.

Il trattamento dei dati contenuti nei log predetti può avvenire esclusivamente in forma anonima, in modo da precludere l'identificazione degli utenti e delle loro attività.

I dati personali contenuti nei log possono essere trattati in forma non anonima solo in via eccezionale ed esclusivamente nelle ipotesi in cui si rilevino evidenze di un utilizzo improprio o illegale, ovvero sia necessario corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria.

4. I dati contenuti nei log saranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza – comunque di regola non superiore a sei mesi – e saranno cancellati periodicamente ed automaticamente dal sistema

## 13. 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.

## 14. INFORMATIVA

Il presente Disciplinare costituisce informativa ai sensi dell'art. 13 del D.lgs. 30 giogno 2003, n. 196 s.m.i. e dell'art. 4, comma 3, della Legge 20 maggio 1970 n. 300 e s.m.i. circa le modalità e finalità del trattamento dei dati personali connessi all'uso delle risorse informatiche e dei servizi di rete.

L'Ente assicura al presente Disciplinare ed ai suoi successivi aggiornamenti la più ampia diffusione presso gli utenti, mediante:

- pubblicazione nella intranet aziendale (own cloud o altro).
- comunicazione del testo a tutti i dipendenti e a coloro che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Ente;
- comunicazione alle rappresentanze sindacali;
- consegna di copia del testo a tutti i futuri dipendenti e a coloro che a vario titolo presteranno servizio o attività per conto e nelle strutture dell'Ente;
- pubblicazione del testo sul sito internet dell'Ente.

Il presente Disciplinare Abroga e sostituisce integralmente tutti i precedenti adottati in materia.

## 15. CLAUSOLA DI REVISIONE

Il presente Disciplinare è aggiornato periodicamente in relazione all'evoluzione tecnologica, organizzativa e della normativa di settore.