
# REGOLAMENTO
# DEL SISTEMA INFORMATIVO PROVINCIALE

# Sommario

## Art. 1. DEFINIZIONI

1. Le parole e le espressioni di seguito indicate hanno il seguente significato:
   - *Amministratore di sistema*: figura professionale individuata dal Titolare dei trattamenti di dati personali della Provincia. Tale figura professionale è generalmente dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software utilizzati dall'ente, le reti locali, gli apparati connessi alla rete e gli apparati di sicurezza.
   - *Antivirus:* un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi.
   - *Backup*: operazione tesa a creare una copia di sicurezza delle informazioni (dati o programmi).
   - *Browser*: in informatica il browser o navigatore è un'applicazione per l'acquisizione, la presentazione e la navigazione di risorse sul web.
   - *Cloud computing o Cloud*: il cloud computing indica, in informatica, un paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita.
   - *Codice identificativo*: codice univoco attribuito dai Sistemi Informativi alle principali Dotazioni hardware, quali personal computer da tavolo, personal computer portatili, tablet, server, switch, router, ecc.; il codice identificativo non è associato al materiale c.d. di consumo, quali mouse, tastiere, ecc.
   - *Data Breach:* 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.
   - *Dati giudiziari*: i dati relativi a condanne penali e reati, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
   - *Dati particolari*: si tratta dei dati c.d. "sensibili", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.
   - *Dati Personali*: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un dato come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Particolarmente importanti sono i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP assegnato in modo permanente ad un PC o ad altro dispositivo hardware in dotazione, il numero di targa di un mezzo di cui si ha la disponibilità);

- *Domain Controller:* sistema che, nell'ambito del Sistema Informativo provinciale, gestisce le richieste di autenticazione per la sicurezza (login, controllo dei permessi, ecc.) e organizza la struttura del sistema in termini di utenti, gruppi e risorse di rete definendo i livelli di accesso alle risorse applicative.
- *Dotazioni informatiche o Dotazioni*: hardware e software nella disponibilità, a qualsiasi titolo, della Provincia di Cuneo.
- *e*-mail: messaggio di posta elettronica.
- *File di Log*: file nel quale vengono registrate cronologicamente informazioni relative alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, base dati);
- *File Server:* sistemi di archiviazione informatica centralizzati o nel cloud adottati dalla Provincia e messi a disposizione degli utenti.
- *Hardware*: parte fisica di dispositivi informatici o di telecomunicazione quali personal computer fissi e portatili, tablet, smartphone, server di rete, stampanti di rete, plotter di rete, switch, router, firewall, gruppi di continuità, timbratrici, telecamere IP, webcam, chiavi USB, hard disk esterni, ecc.
- *Hard Disk*: dispositivo di memoria di massa che utilizza uno o più dischi magnetici per l'archiviazione dei dati.
- *Interessati*: persone fisiche, identificate o identificabili, alle quali si riferiscono i dati personali.
- *Internet*: rete di collegamenti informatici a livello planetario che permette la connessione e la comunicazione tra loro di reti locali di computer e banche dati, rendendone disponibili agli utenti le informazioni nella forma di ipertesti, immagini, filmati, musica e servizi.
- *Intranet*: rete interna aziendale che utilizza i protocolli di comunicazione di Internet, a cui però possono avere accesso solo utenti riconosciuti; la definizione include anche il sito web interno intranet.provincia.cuneo.it;
- *Login*: attività volta ad identificare una utenza per l'accesso ad un computer o a un software tramite inserimento di User ID e Password.
- *Logout*: attività volta a disconnettere una utenza dall'accesso ad un computer o a un software.
- *Mailing list* o *Liste di distribuzione o Caselle postali:* sistema organizzato per la condivisione via e-mail di messaggi a più persone.
- *Normativa Applicabile:* normativa e regolamenti elencati al precedente punto 3 e tutti gli ulteriori provvedimenti e linee guida del Garante comunque applicabili.
- *Password*: parola segreta associata ad un User ID.
- *Personal computer (di seguito "PC"):* computer da tavolo o portatile.
- *Peer-to-Peer*: tipologia di rete informatica caratterizzata da condivisione diretta di risorse tra i nodi della stessa che sono organizzati in modo non gerarchico.
- *Portale internet istituzionale*: www.provincia.cuneo.it
- *Postazione o postazione di lavoro:* è costituita da un personal computer – da tavolo e/o portatile – e da dispositivi e periferiche, a seconda delle specifiche esigenze lavorative, quali ad esempio: tablet, monitor, mouse, tastiera, cavi di alimentazione, cavi di rete, cavi USB, webcam, cuffie, microfoni, lettori smart card.
- *Responsabile del trattamento:* la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno alla Provincia, che tratta dati personali per conto della stessa, ai sensi dell'art. 28 GDPR.

- *Responsabile della Protezione dei Dati:* Responsabile della protezione dei dati previsto dall'art. 37 del GDPR, nonché figura di contatto per il Garante. E' sinonimo di *Data Protection Officier* o D.P.O.
- *Responsabile della struttura:* il Dirigente del Settore/Ufficio o il dipendente a cui è assegnato un incarico di responsabile di Posizione Organizzativa di un Ufficio.
- *Server*: componente informatica, fisica o virtuale, che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete.
- *Sistemi Informativi*: l'unità organizzativa della Provincia di Cuneo preposta alla gestione del sistema informativo provinciale.
- *Sistema informativo provinciale*: consiste nell'insieme composto dalle Dotazioni informatiche e dall'infrastruttura di telecomunicazione della rete locale, extranet ed internet ed è finalizzato alla gestione, raccolta, registrazione, elaborazione, conservazione e comunicazione del patrimonio informativo della Provincia per l'esercizio dell'azione amministrativa e l'erogazione di servizi a utenti interni ed esterni.
- *Social media*: sono servizi che offrono la possibilità di condividere su Internet contenuti testuali, immagini, audio e video; i più noti social media includono le seguenti piattaforme (elenco non esaustivo): X, Instagram, Facebook, LinkedIn, TikTok, Wikipedia, Youtube, WhatsApp, WeChat, Telegram e Signal.
- *Software:* programma o un insieme di programmi o applicazione informatica.
- *Software aziendale centralizzato:* programma o insieme di programmi o applicazione informatica utilizzata da più utenti e volta a risolvere specifiche esigenze professionali dell'ente (ad es. gestione delle risorse umane, economica, patrimoniale, ecc.) gestito centralmente;
- *Software open source*: con software open source (in italiano software a sorgente aperto), in informatica, si indica un tipo di software libero da vincoli di copyright o altra natura, nonché il suo modello di sviluppo o distribuzione.
- *Titolare del trattamento:* 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 dei 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 consulenza, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- *User ID:* identificativo unico associato ad una persona per l'accesso al sistema informativo provinciale;
- *Virus*: un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, potendo provocare danni sia al software che all'hardware.
- *Wi-fi*: sistema di comunicazione tra dispositivi elettronici basato su standard internazionali che non fa uso di cavi.

## Art. 2. PRINCIPALI RIFERIMENTI NORMATIVI E REGOLAMENTI PROVINCIALI

1. Nella definizione delle norme comportamentali da osservare nel Regolamento si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare del:
   a) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("GDPR");
   b) Decreto legislativo 10 agosto 2018, n. 101, “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016”;
   c) Provvedimento del Garante del 1° marzo 2007, “Lavoro: le linee guida del Garante per posta elettronica e Internet”, pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
   d) Provvedimento del Garante del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, pubblicato in Gazzetta Ufficiale n. 300 del 24 dicembre 2008 e s.m.i.;
   e) Provvedimento del Garante “Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali – 13 ottobre 2008”, pubblicato nella G.U. n. 287 del 9 dicembre 2008;
   f) 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");
   g) Legge 22 aprile 1941 n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio";
   h) le circolari dell’Agenzia per l’Italia Digitale (AGID), in particolare la circ. 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)”;
   i) il D.P.R. 16/04/2013, n. 62 “Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165”;
   j) Il vigente Contratto Collettivo Nazionale di Lavoro e Contratto Collettivo Decentrato Integrativo.
   k) I vigenti Regolamenti adottati dalla Provincia di Cuneo.

## Art. 3. PREMESSA

1. La Provincia di Cuneo (di seguito "Provincia") adotta il Regolamento del sistema informativo provinciale per fornire un quadro preciso di indicazioni in merito ai criteri ed alle modalità d’assegnazione e di utilizzo delle Dotazioni informatiche.
2. L’utilizzo delle Dotazioni informatiche deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza, che devono costantemente uniformare e caratterizzare la condotta generale ed i singoli comportamenti di tutti i soggetti autorizzati al loro utilizzo.
3. E’ responsabilità di tutti i soggetti che utilizzano le Dotazioni informatiche messe a disposizione dalla Provincia di Cuneo applicare e rispettare puntualmente le disposizioni del presente Regolamento.

## Art. 4. SCOPO

1. Il presente Regolamento persegue i seguenti scopi:
   a) garantire la sicurezza, la disponibilità e l'integrità del sistema informativo provinciale, inclusi i dati archiviati digitalmente;
   b) mantenere in efficienza, ottimizzare l'uso e prevenire utilizzi indebiti delle Dotazioni informatiche;

c) evitare che gli utenti possano esporre sé stessi e/o la Provincia a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito delle Dotazioni informatiche, nonché esporre la Provincia a conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine;
d) recepire e dare attuazione alle disposizioni normative e ai principi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito anche solo "GDPR"), nonché dei Provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante").

2. Non rientra tra gli scopi del presente Regolamento il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei suoi dipendenti, che rimangono strettamente vietati e non consentiti.

## Art. 5. AMBITO DI APPLICAZIONE

1. Il Regolamento si applica ai seguenti soggetti, di seguito complessivamente denominati "utenti":

a) i dipendenti, che nel contesto del presente Regolamento includono sia i dipendenti della Provincia di Cuneo, che il personale distaccato presso la Provincia di Cuneo da altri Enti pubblici con qualsivoglia tipo di accordo o modalità amministrativa;
b) i titolari di cariche politiche della Provincia di Cuneo;
c) i soggetti esterni all'Amministrazione (ad esempio collaboratori esterni, stagisti, borsisti, studenti, consulenti, fornitori, tecnici di ditte esterne) ai quali verranno espressamente riconosciute applicabili le disposizioni del presente Regolamento.

2. Rimane ferma, in ogni caso, l'inapplicabilità agli utenti che non rientrano nella categoria dei dipendenti di cui al precedente punto 5.1.a di ogni riferimento relativo ai profili disciplinari e, più in generale, di ogni ulteriore previsione e/o normativa richiamata nel Regolamento che presupponga lo svolgimento di attività in regime di subordinazione.

## Art. 6. DISPOSIZIONI RIGUARDANTI L'ACCESSO AL SISTEMA INFORMATIVO PROVINCIALE

1. Contestualmente all'inizio del rapporto di lavoro dei dipendenti (punto 5.1.a) o alla data indicata nella richiesta di abilitazione dei titolari di cariche politiche (punto 5.1.b), viene creata dagli Amministratori di Sistema un'utenza nel Domain Controller.
2. L'utenza nel Domain Controller per gli utenti di cui al precedente punto 5.1.c è creata su richiesta del Dirigente responsabile della struttura in cui opereranno fornendo il nome, il cognome, la data di nascita, la data di inizio e conclusione del rapporto con l'Amministrazione, le abilitazioni richieste.
3. In funzione delle specifiche esigenze di servizio o di funzione di ciascun utente, sono configurabili le abilitazioni relative:
   a) alla rete provinciale;
   b) alla casella di posta elettronica personale;
   c) alla posta elettronica istituzionale, incluse le liste di distribuzione o caselle postali dedicate;
   d) al file server per l'accesso alle cartelle di servizio;
   e) al file server per l'accesso alle cartelle personali;
   f) alla intranet provinciale;
   g) ai software applicativi.

Ulteriori abilitazioni avvengono su richiesta del Responsabile della struttura di appartenenza.

4. L'accesso al sistema informativo provinciale è, di norma, autorizzato dal lunedì al venerdì dalle ore 7 alle ore 20.
5. Gli utenti che, per esigenze di servizio, devono poter accedere al sistema informativo provinciale anche al di fuori dell'orario indicato al punto precedente, dovranno essere preventivamente autorizzati dal Segretario Generale o dal Dirigente da cui dipendono.

## Art. 7. ACQUISIZIONE E MESSA A DISPOSIZIONE DELLE DOTAZIONI INFORMATICHE

1. Le assegnazioni delle Dotazioni agli utenti avviene sulla base delle esigenze generali espresse dalla Provincia o da esigenze specifiche espresse dai Responsabili delle strutture.
2. Tutte le Dotazioni, sia hardware che software con licenza d'uso a titolo oneroso o di proprietà in uso nel sistema informativo provinciale, devono sempre essere acquisite in accordo con le specifiche tecniche fornite dai Sistemi Informativi.
3. I software open source o i software utilizzabili gratuitamente dagli utenti, anch'essi facenti parte delle Dotazioni informatiche, sono preventivamente vagliati e messi a disposizione dagli Amministratori di rete nella intranet dell'Ente, oppure fornendo direttamente il link internet da cui scaricarlo, oppure tramite installazione manuale o automatica da parte degli Amministratori di rete sulla postazione di lavoro.
4. I servizi informatici accessibili con un browser via internet, erogati da terzi a titolo gratuito o oneroso e che non necessitano integrazioni con il sistema informativo provinciale, possono essere messi a disposizione dai Settori ed Uffici previa verifica tecnica degli Amministratori di rete.

## Art. 8. DISPOSIZIONI RIGUARDANTI MESSA A DISPOSIZIONE DELLE DOTAZIONI HARDWARE

### 8.1 POSTAZIONE DI LAVORO

1. Di norma, a ciascun utente viene assegnata una sola postazione di lavoro presso la Provincia e, per i soli utenti autorizzati dal proprio Dirigente, un PC portatile e relativi accessori.
2. Richieste di ulteriori assegnazioni, in quanto deroganti al suddetto principio, devono essere motivate dal Responsabile della struttura ed autorizzate dai Sistemi Informativi.
3. L'assegnazione della postazione di lavoro, o di un suo componente o accessorio, ad un utente viene effettuata direttamente dal Responsabile della struttura se l'attrezzatura è già presente presso l'ufficio o il settore, previa comunicazione via e-mail all'assistenza informatica.
4. Nel caso sia necessaria l'assegnazione di nuova postazione di lavoro, il Responsabile della struttura ne fa richiesta ai Sistemi informativi tramite messaggio di posta elettronica inviato all'assistenza informatica. Se è disponibile, previa verifica tecnica della richiesta, questa verrà messa a disposizione, oppure acquisita alla prima occasione utile.
5. Gli utenti che svolgono funzioni che non richiedono un'assegnazione personale della postazione di lavoro utilizzano postazioni in condivisione con altri utenti sulla base dell'organizzazione definita dalle rispettive strutture.

6. In caso di trasferimento dell'utente ad altro ufficio o ad altra sede di lavoro dell'ente, di norma, la postazione viene trasferita contestualmente. Nel caso in cui la postazione di lavoro abbia caratteristiche tecniche particolari legate alle specifiche funzioni delle strutture coinvolte, i Sistemi Informativi valutano, sentite le strutture stesse, soluzioni differenti.
7. In caso di cessazione del rapporto di lavoro, di assenza o trasferimenti temporanei di lunga durata ad altri enti, e in qualsiasi caso di sostituzione della postazione di lavoro, la postazione precedentemente assegnata all'utente ritorna nella disponibilità dei Sistemi Informativi che decidono in merito al suo riutilizzo o dismissione. In tali casi è compito del Responsabile della struttura comunicare tempestivamente la dismissione delle Dotazioni tramite segnalazione via posta elettronica all'assistenza informatica.
8. Nei casi di cui al punto 7 il Dirigente responsabile può richiedere ai Sistemi Informativi di recuperare dalle postazioni di lavoro, prima della dismissione, i dati strettamente necessari al proprio Settore.

### 8.2 DISPOSITIVI DI STAMPA

1. Ai fini del contenimento dei costi e in considerazione degli obblighi di dematerializzazione in atto nella Pubblica Amministrazione, nonché dell'inquinamento ambientale derivante dalle stesse, le stampanti multifunzione ed i plotter di rete sono collocati in aree comuni, sono utilizzabili da gruppi definiti di utenti e non sono legate a singole strutture organizzative.
2. Gli Amministratori di Sistema abilitano l'accesso ai dispositivi di stampa in funzione delle esigenze lavorative di ciascun utente o di gruppi di utenti omogenei.

### 8.3 DISPOSITIVI DI TELEFONIA MOBILE E TABLET

1. I dispositivi di telefonia mobile e tablet sono assegnati ai dipendenti dai Dirigenti delle strutture esclusivamente per esigenze di servizio.
2. Nel caso di dispositivi di telefonia mobile o di tablet destinati a cariche politiche, la richiesta è formulata dal Segretario Generale.
3. I dispositivi di telefonia mobile ed i tablet sono acquisiti dai Sistemi Informativi o forniti nell'ambito del contratto di fornitura del servizio di telefonia mobile in vigore.
4. I dispositivi di telefonia mobile ed i tablet sono configurati dagli Amministratori di Sistema. Le configurazioni non possono essere variate dagli utenti.
5. Per particolari esigenze di servizio, i dispositivi di telefonia mobile o i tablet possono essere messi a disposizione di più utenti.
6. La responsabilità dell'utilizzo dei dispositivi di telefonia mobile e dei tablet è sempre in capo agli utenti che ne fanno uso.

## Art. 9. DISPOSIZIONI RIGUARDANTI LE MODALITÀ D'USO DELLE DOTAZIONI INFORMATICHE

### 9.1 NORME GENERALI DI COMPORTAMENTO

1. All'utente del sistema informativo provinciale è consentito l'utilizzo degli strumenti informatici forniti dall'Amministrazione provinciale per poter assolvere alle incombenze personali senza doversi

allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

2. Gli utenti sono tenuti ad utilizzare le Dotazioni informatiche messe a loro disposizione con diligenza, adottando comportamenti idonei a non causare danni alle stesse.
3. Gli utenti dovranno osservare gli obblighi specifici di seguito riportati:
   a) è fatto divieto di cedere a terzi le Dotazioni informatiche, o loro componenti, e comunque di consentirne l'utilizzo da parte di terzi non autorizzati dalla Provincia;
   b) è fatto divieto di manomettere in qualsiasi le Dotazioni informatiche assegnate;
   c) è fatto divieto di impiegare le Dotazioni informatiche per finalità diverse da quelle per le quali sono state progettate o utilizzarle per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all'ente;
   d) è fatto obbligo di segnalare eventuali furti o smarrimenti delle Dotazioni informatiche così come indicato al paragrafo 9.2.J;
   e) è fatto obbligo di segnalare ogni anomalia o malfunzionamento riguardante le Dotazioni informatiche all'assistenza informatica provinciale.

## 9.2 NORME GENERALI PER LA SICUREZZA

1. L'integrità e la disponibilità delle informazioni e dei dati, ivi inclusi i dati personali, sono garantite solo quando gli stessi sono memorizzati nel software aziendale centralizzato e nei file server messi a disposizione dalla Provincia, oggetto di sistemi di protezione, monitoraggio e backup.
2. Le informazioni ed i dati presenti sui PC in dotazione agli utenti non sono oggetto di backup.
3. Per garantire la sicurezza, la disponibilità e la riservatezza dei dati è fatto obbligo agli utenti di:
   a) mantenere la riservatezza delle proprie credenziali d'accesso alle Dotazioni informatiche, al sistema informativo provinciale nel suo complesso e ai singoli applicativi;
   b) salvare documenti e dati nelle cartelle di rete sul file server relativo alla struttura di appartenenza;
   c) salvare documenti contenenti dati personali particolari o dati giudiziari nelle cartelle di rete criptate sul file server relativo alla struttura di appartenenza;
   d) eventuali dati strettamente personali, inerenti comunque all'attività lavorativa, possono essere salvati nella cartella di rete riservata a ciascun utente presente sul file server;
   e) archiviare le informazioni e i dati esclusivamente necessari all'attività lavorativa;
   f) costituisce buona regola la pulizia periodica degli archivi, da eseguirsi almeno ogni 6 mesi, con cancellazione dei file obsoleti o inutili; particolare attenzione va prestata alla duplicazione dei dati, al fine di evitare un'archiviazione ridondante;
   g) effettuare il logout dalla propria postazione di lavoro al termine della giornata lavorativa e bloccarla in caso di allontanamento dalla stessa;
   h) presidiare l'intero processo di stampa, fotocopia, scansione o trasmissione via fax di documenti, al fine di impedire la volontaria o accidentale diffusione di dati personali o la perdita di riservatezza sulle informazioni contenute nei documenti stessi; allo stesso scopo, è dovere degli utenti prelevare immediatamente i fogli riprodotti da stampanti, fotocopiatrici e fax e cancellare dalle cartelle condivise di destinazione delle scansioni i file creati;
   i) in caso di trasferimento ad altra struttura dell'ente, prima dello spostamento eliminare dalla postazione, dalle cartelle di rete personali e dalla posta elettronica eventuali file, documenti o messaggi contenenti dati che non si è più autorizzati a trattare e che non siano di interesse per la

struttura di appartenenza; i dati di interesse per la struttura di appartenenza dovranno essere caricati sulle cartelle di rete sul file server prima del trasferimento ad altra struttura dell'ente;

j) qualora si verificasse il furto o lo smarrimento di una dotazione informatica o di telecomunicazione, comunicare immediatamente, anche per le vie brevi, e comunque entro 24 ore dalla scoperta l'accaduto al proprio Dirigente, sporgere denuncia alle Autorità competenti e seguire la procedura di gestione dei data breach pubblicata in intranet.

3. E' fatto obbligo di raccogliere tempestivamente tutti i documenti stampati che non sono più richiesti o necessari e di provvedere alla loro definitiva eliminazione. Tali documenti, nel caso contengano dati personali o riservati, devono sempre essere resi non intelligibili.

## 9.3 NORME PER L'UTILIZZO DELLA POSTAZIONE DI LAVORO

1. L'assegnazione di Dotazioni informatiche al dipendente è finalizzata allo svolgimento dell'attività lavorativa. In caso di utilizzo difforme, l'utente sarà ritenuto esclusivo responsabile per ogni eventuale danno che dovesse derivarne.
2. Le Dotazioni informatiche vengono installate, configurate, connesse alla rete locale e/o alla rete wireless della Provincia di Cuneo ed aggiornate dagli Amministratori di Sistema.
3. Eventuali modifiche alla configurazione iniziale delle Dotazioni informatiche in uso agli utenti devono essere preventivamente richieste e motivate dal Dirigente. Solo nel caso in cui la verifica della fattibilità tecnica e del mantenimento di un livello di sicurezza almeno pari a quello in essere abbia esito positivo, gli Amministratori di Sistema procederanno, previo assenso del Dirigente dei Sistemi Informativi, ad apportare le modifiche della configurazione dell'hardware e del software che si rendono necessarie.
4. Nel caso sia necessario portare qualsiasi Dotazione informatica fuori della sede di lavoro (ad es. in caso di eventi, corsi, ecc.) è fatto obbligo agli utenti di prendere tutte le precauzioni affinché non venga smarrita, danneggiata o rubata, nonché di prestare assoluta attenzione a non lasciarla mai incustodita e di conservarla in luoghi protetti.
5. Le seguenti attività sono espressamente proibite agli utenti:
   a) modificare la configurazione hardware in dotazione, aggiungendo o rimuovendo componenti;
   b) installare e/o configurare apparati di rete quali, a titolo di esempio non esaustivo, firewall, router, modem, oppure schede di rete per la connettività alla rete locale o alla rete wireless di PC, PC portatili, tablet o altro hardware connesso alla rete provinciale;
   c) qualora le Dotazioni informatiche (ad esempio un PC portatile o un tablet) siano dotate di modem, antenna wi-fi, o possano connettersi ad internet tramite un altro dispositivo per trasmissione dati, o tramite la rete cellulare, è severamente vietato l'utilizzo di questi dispositivi quando contemporaneamente sono connessi alla rete locale dell'ente sia in modalità wireless (es. wi-fi), che fisica (es. con il cavo di rete);
   d) modificare la configurazione software in dotazione, installare/effettuare download di software/applicativi non autorizzati dai Sistemi Informativi;
   e) eliminare un programma o file installato legalmente in modo tale da impedire od ostacolare le normali operazioni, ivi inclusa la disattivazione dei sistemi di sicurezza;
   f) acquisire, utilizzare, duplicare software illegalmente.
6. Nel caso in cui gli utenti vengano a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai software e/o ai sistemi, dovranno darne tempestivamente comunicazione all'assistenza informatica.

7. È proibita ogni attività finalizzata a collaudare la sicurezza del sistema informativo provinciale, salvo esplicita autorizzazione fornita dal Dirigente dei Sistemi Informativi.

## 9.4 NORME PER L'ACCESSO AL SISTEMA INFORMATIVO PROVINCIALE E LA GESTIONE DELLE CREDENZIALI

1. L'accesso al sistema informativo provinciale è sottoposto a procedure di identificazione personale (login) tramite Domain Controller basate sull'utilizzo di credenziali di autenticazione rilasciate dagli Amministratori di Sistema.
2. Le credenziali di autenticazione personali sono composte da un identificativo univoco (User ID) nella forma COGNOME_NOME e da una parola segreta (password) necessari al riconoscimento della identità degli utenti da parte del sistema installato sulle Dotazioni informatiche e/o del software in uso.
3. I casi di omonimia sono gestititi dagli Amministratori di Sistema differenziando opportunamente gli identificativi.
4. Le credenziali di autenticazione sono segrete e strettamente personali.
5. L'utente è tenuto:
   a) a modificare la password al momento del primo utilizzo e ogniqualvolta richiesto dalle procedure automatiche di cambio password impostate con scadenza almeno semestrale, nonché tutte le volte ritenga siano venuti meno i requisiti di riservatezza;
   b) a non comunicarle in alcun caso ad altri soggetti;
   c) a non inserirle in messaggi di posta elettronica o trasmetterle attraverso qualsiasi altra forma di comunicazione elettronica;
   d) a non salvarle su strumenti o documenti informatici che non siano protetti a loro volta da apposite credenziali;
   e) a non trascriverle su fogli, biglietti, post-it o su oggetti, soprattutto se posti nelle vicinanze del PC o sulla scrivania di lavoro;
6. Nella scelta delle password, l'utente è tenuto a rispettate le seguenti regole:
   a) deve essere composta da almeno 8 caratteri;
   b) deve contenere almeno 3 delle seguenti caratteristiche: una lettera minuscola, una lettera maiuscola, un numero o un carattere speciale;
   c) non si può impostare una password che sia uguale a una delle ultime password inserite;
   d) non deve contenere riferimenti personali, anche se in forma parziale, come il proprio nome, la data di nascita, il numero di matricola e qualsiasi altro dato riconducibile all'utente o alla sua storia personale;
7. I sistemi di autenticazione dei sistemi informativi provinciali possono implementare ulteriori regole di accesso che l'utente è tenuto a rispettare. E' il caso, ad esempio, della regole di accesso al sistema informativo provinciale da remoto tramite un PC portatile fornito dalla Provincia, oppure della connessione alla rete wireless provinciale.
8. L'utente è responsabile di qualsiasi azione o attività svolta tramite l'utilizzo delle credenziali personali a lui assegnate.
9. Per ragioni di sicurezza, gli Amministratori di Sistema possono disattivare temporaneamente l'accesso di un utente fino al ripristino delle condizioni di sicurezza, dandone comunicazione al Dirigente dei Sistemi Informativi ed all'utente interessato.

## 9.5 NORME PER L'ACCESSO AL SISTEMA INFORMATIVO PROVINCIALE DA REMOTO

1. L'autorizzazione all'accesso al sistema informativo provinciale da remoto è consentita ai dipendenti in possesso di autorizzazione del proprio Dirigente a prestare l'attività lavorativa con tale modalità.
2. Il Segretario Generale, i Dirigenti e gli Amministratori di Sistema sono sempre autorizzati ad accedere al sistema informativo provinciale da remoto.
3. I dipendenti che accedono da remoto al sistema informativo provinciale sono, di norma, dotati di un PC portatile o un tablet e accessori fornito dalla Provincia e sono abilitati all'accesso dagli Amministratori di Sistema.
4. L'accesso da remoto è realizzato con una connessione criptata resa disponibile da uno o più software forniti dai Sistemi Informativi, che abilitano una rete privata virtuale provvista di apposito certificato digitale rilasciato dai Sistemi Informativi.
5. L'autenticazione degli utenti sulla rete privata virtuale è effettuato tramite le proprie credenziali di autenticazione al sistema informativo provinciale.
6. Di norma, ad ogni utente è consentita solamente la connessione da remoto al PC della propria postazione di lavoro presso gli uffici provinciali.
7. Gli Amministratori di Sistema possono, per esigenze di lavorative, accedere da remoto ai file server del sistema informativo provinciale ed alle postazioni di lavoro degli utenti cui prestano assistenza informatica.
8. Tutti i dipendenti e i titolari di cariche politiche presso la Provincia di Cuneo possono accedere ai servizi loro riservati erogati attraverso il portale internet istituzionale.

## 9.6 NORME PER L'UTILIZZO DI INTERNET

1. Fatto salvo quanto previsto all'art. 9.1 c.1, la Provincia di Cuneo consente agli utenti l'accesso alla rete internet per esclusivi scopi lavorativi.
2. Al fine di garantire un appropriato utilizzo della rete internet, ogni utente deve rispettare le seguenti regole o norme comportamentali:

    a) è consentita la navigazione in internet solo su siti contenenti informazioni necessarie o utili all'attività lavorativa o, comunque, all'acquisizione di notizie utili alla propria formazione/informazione professionale;
    b) l'utente non è autorizzato all'installazione di programmi o di software per la fruizione di servizi e contenuti;
    c) l'utente non è autorizzato ad effettuare il download di software, file musicali e video con finalità estranee all'attività lavorativa;
    d) l'utente deve rispettare le norme in materia di diritto di autore;
    e) l'utente non è autorizzato ad accedere a servizi di condivisione di file in modalità peer-to-peer;
    f) l'utente non deve utilizzare sistemi per l'offuscamento della connessione con la finalità di rendere nascosta la propria identità nella rete, in particolare è vietato l'utilizzo di servizi o software di anonimizzazione;
    g) l'utente è personalmente responsabile della propria condotta nell'utilizzo della rete internet.

3. La Provincia filtra in modo automatico il traffico internet bloccando la navigazione su siti e/o categorie di siti i cui contenuti sono ritenuti come estranei alle proprie attività. Rientrano in questa categoria, a titolo di esempio non esaustivo, siti internet con contenuti pornografici, siti di incontri on-line, siti pubblicitari, siti che premettono il download di file illegali o virus o malware, siti con frodi bancarie o phishing.

## 9.7 NORME PER L'UTILIZZO DEI MEZZI DI INFORMAZIONE E DEI SOCIAL MEDIA

1. Durante l'orario di servizio non è permesso ai dipendenti, salvo che per motivi lavorativi, professionali e formativi, partecipare --tramite l'accesso ad internet della Provincia-- a forum, utilizzare chat line, bacheche elettroniche o social media, anche usando pseudonimi.
2. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Provincia di Cuneo.
3. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine della Provincia di Cuneo o della pubblica amministrazione in generale.
4. Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.
5. Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 14 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

## 9.8 NORME PER L'UTILIZZO DELLA POSTA ELETTRONICA

1. Il servizio di posta elettronica messo a disposizione dalla Provincia è uno dei mezzi istituzionali di comunicazione adottati dall'Ente.
2. L'utilizzo di caselle di posta elettronica istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione della Provincia di Cuneo. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui l'utente del sistema informativo provinciale, per qualsiasi ragione, non possa accedere alla casella di posta elettronica istituzionale.
3. L'invio e la ricezione di messaggi di posta elettronica da parte degli utenti del sistema informativo provinciale a soggetti interni ed esterni all'Amministrazione è consentito per lo scambio di comunicazioni, documenti e dati utili per scopi lavorativi, organizzativi, di comunicazione e di gestione del personale dell'Ente.
4. Ad ogni utente cui viene assegnata una casella di posta elettronica istituzionale personale denominata: cognome_nome@provincia.cuneo.it.
5. I casi di omonimia sono gestititi dagli Amministratori di Sistema differenziando opportunamente le caselle di posta elettronica personali.

6. Ad ogni settore ed ufficio sono assegnate delle liste di distribuzione di posta elettronica istituzionali, per comunicazioni informali provenienti dall'esterno ed a cui accedono i dipendenti individuati dal Dirigente responsabile, e delle liste di distribuzione di posta elettronica ad uso interno, in cui sono presenti tutti i membri dell'unità organizzativa.
7. Su richiesta motivata dei Responsabili di struttura, vengono generate ulteriori liste di distribuzione o caselle di posta elettronica per la gestione condivisa di indirizzi di posta istituzionali.
8. L'invio di messaggi di posta elettronica agli utenti del sistema informativo provinciale ed a soggetti esterni all'Amministrazione è altresì consentito:
   a) ai membri della Rappresentanza Sindacale Unitaria della Provincia tramite la casella di posta elettronica rsu@provincia.cuneo.it assegnata dalla Provincia;
   b) ai membri del direttivo del Centro ricreativo provinciale tramite la casella di posta elettronica centroricreativo@provincia.cuneo.it assegnata dalla Provincia.
9. L'utente del sistema informativo provinciale è responsabile del contenuto dei messaggi inviati, nonché di garantire la riservatezza delle credenziali di accesso.
10. Ciascun messaggio in uscita deve consentire l'identificazione dell'utente del sistema informativo mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile. A seconda del programma di gestione della posta elettronica utilizzato, l'utente dovrà configurare il testo per la firma in formato HTML oppure, in alternativa, il biglietto da visita elettronico (vCard), contenente i seguenti dati minimi: cognome e nome, settore di appartenenza, ufficio di appartenenza, numero di telefono fisso e/o del cellulare di servizio al quale il medesimo è reperibile.
11. Per un corretto utilizzo della posta elettronica ogni utente dovrà rispettare le seguenti prescrizioni:
    a) è vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'Amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'Amministrazione;
    b) non violare il segreto della corrispondenza personale e il diritto alla riservatezza;
    c) non trasmettere messaggi di posta elettronica che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo.
    d) non è consentito inviare tramite posta elettronica messaggi pubblicitari e/o promozionali;
    e) non è consentito trasmettere materiale e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
    f) non è consentito l'utilizzo di programmi di sicurezza e/o di crittografia non previsti esplicitamente dalle procedure di sicurezza messe in atto dal Settore Sistemi Informativi.
    g) non aprire documenti, eseguire programmi, seguire link a siti internet, contenuti in messaggi di provenienza incerta;
    h) è necessario verificare periodicamente l'archivio della propria casella di posta elettronica conservando solo la corrispondenza strettamente necessaria alla propria attività e cancellando la restante;
    i) i messaggi di posta elettronica vanno inviati solo ai destinatari oggettivamente interessati alla comunicazione, cercando di limitarne il più possibile il numero; in particolare, è vietata la diffusione di "catene" di ogni genere e tipo;
    j) al fine di limitare l'occupazione di spazio è necessario evitare l'invio documenti di rilevante dimensione a una pluralità di destinatari, preferendo sistemi di condivisione dei documenti;
    k) evitare di iscriversi a liste di distribuzione (c.d. "mailing list") esterne salvo che queste non siano utili per l'espletamento della propria attività lavorativa;

l) non utilizzare gli indirizzi di posta elettronica assegnati dalla Provincia per la partecipazione a dibattiti, chat, forum, social network o mailing-list per uso privato.

12. I messaggi di posta elettronica possono essere letti dagli utenti tramite i client di posta configurati dagli Amministratori di rete sulla postazione di lavoro e sui cellulari, oppure con l'apposito applicativo Webmail raggiungibile dal portale Internet della Provincia di Cuneo. Nel caso di accesso alla posta elettronica tramite il client di posta presente sulla postazione di lavoro, di norma, una volta scaricati i messaggi vengono cancellati dal server. E' responsabilità dell'utente il salvataggio dei messaggi di posta elettronica ritenuti importanti sulle cartelle di rete al fine di permetterne il backup automatico. I messaggi meno recenti residenti sul server di posta possono essere cancellati, senza preavviso, anche in seguito a operazioni di manutenzione o di aggiornamento del software.
13. Al fine di assicurare la disponibilità del contenuto della casella di posta elettronica in caso di improvvisa o prolungata assenza degli utenti o di un loro impedimento, l'accesso alla predetta casella di posta elettronica potrà essere effettuato dall'Amministratore di Sistema. Alla prima occasione utile, sarà cura dell'Amministratore di Sistema informare di tali attività l'utente interessato.
14. Ad ogni e-mail inviata attraverso il sistema di posta elettronica della Provincia viene automaticamente aggiunta una nota finale riportante un avviso di riservatezza circa le informazioni contenute nella comunicazione ricevuta e le modalità di gestione delle stesse in caso di erronea trasmissione.
15. In tutti i casi in cui è necessario che la trasmissione di documenti, atti e quant'altro avvenga con modalità elettroniche ed acquisti valore giuridico, attraverso una certificazione dell'invio e della consegna dei contenuti trasmessi, si deve utilizzare la Posta Elettronica Certificata (P.E.C.) dell'Ente.

## 9.9 NORME PER L'UTILIZZO DEI DISPOSITIVI DI MEMORIA PORTATILI

1. Ai dipendenti, in caso di necessità, può essere assegnato un dispositivo di memoria portatile (ad es. una chiave USB).
2. Agli assegnatari di dispositivi di memoria portatile è richiesto di:
   a) non utilizzare supporti di memoria portatili per archiviare informazioni contenenti dati personali; in caso effettiva necessità, si prega di prendere contatto preventivamente con gli Amministratori di Sistema per valutare idonee soluzioni tecniche, inclusa la cifratura;
   b) custodire sempre i dispositivi di memoria portatili in idonei archivi (es. armadio o cassettiera) chiusi a chiave;
   c) non consegnare a terzi i dispositivi di memoria portatili su cui sono presenti dati personali o riservati.
3. Tutti i dispositivi di memoria portatili sono automaticamente scansionati dall'antivirus non appena connessi ai personal computer del sistema informativo provinciale.
4. E' vietato utilizzare dispositivi di memoria portatili personali sulle Dotazioni informatiche fornite dall'Ente.

## 9.10 NORME PER IL REIMPIEGO, RICICLO O DISMISSIONE DELLE DOTAZIONI HARDWARE

1. I dipendenti sono tenuti ad applicare misure volte a prevenire accessi non consentiti ai dati, personali o meno, nel reimpiego, riciclo o smaltimento delle Dotazioni hardware.
2. In caso di reimpiego (ad es. assegnazione ad altro utente) o riciclo (ad es. donazione o cessione in comodato d'uso a scuole o associazioni) di Dotazioni informatiche quali PC e server fisici, le misure e gli accorgimenti volte a prevenire accessi non consentiti agli eventuali dati personali in esse contenuti

prevedono la completa sovrascrittura dei dati presenti sul disco fisso attraverso l'installazione di una nuova immagine del sistema operativo. Questa operazione è svolta dagli Amministratori di Sistema.

3. Nel caso di reimpiego di un dispositivo di memoria portatile riscrivibile (ad es. chiave USB), l'utente cui è stato assegnato dovrà provvedere autonomamente alla formattazione del dispositivo prima della destinazione ad un nuovo soggetto.
4. In caso di smaltimento di Dotazioni informatiche hardware, quali ad esempio i PC, i server fisici o i dispositivi di memoria portatile, le misure volte a prevenire accessi non consentiti ai dati avviene attraverso:
   a) sistemi di punzonatura o deformazione meccanica dei dischi fissi delle postazioni di lavoro, server o altro dispositivo dotato di memoria interna permanente;
   b) la distruzione fisica o la disintegrazione di dispositivi di memoria portatili (ad es. supporti ottici CD-ROM/DVD-ROM e chiavi USB);

   Entrambe le operazioni di cui ai punti a) e b) sono svolte dagli Amministratori di Sistema.

## 9.11 NORME PER L'UTILIZZO DELLE DOTAZIONI INFORMATICHE PERSONALI

1. L'utilizzo da parte dei dipendenti di Dotazioni informatiche personali non fornite dall'Ente per l'accesso al sistema informativo provinciale è vietata, fatto salvo richieste motivate da parte del Segretario Generale o dei Dirigenti.
2. Nei casi delle richieste di cui al punto 1, gli Amministratori di Sistema procedono alla verifica della Dotazione informatica e, nel caso in cui soddisfi analoghi requisiti di sicurezza delle Dotazioni informatiche fornite dall'Ente (ad esempio, con sistema operativo ed antivirus aggiornati, assenza di software che possano pregiudicare la sicurezza informatica, ecc.), la configurano per l'accesso al sistema informativo provinciale o a parte di esso (ad esempio per il solo accesso ad internet o alla posta elettronica dell'Ente).
3. Per ragioni di sicurezza, gli Amministratori di Sistema possono sospendere l'accesso al sistema informativo provinciale delle Dotazioni informatiche di cui al punto 1, dandone comunicazione al Dirigente dei Sistemi Informativi ed all'utente interessato.
4. L'utente proprietario della Dotazione informatica di cui al punto 1 manleva e tiene indenne da qualsiasi rivendicazione, azione legale e/o richiesta di risarcimento derivante dall'accesso e/o dalla configurazione e/o dalla sospensione all'accesso al sistema informativo provinciale della Dotazione informatica, sia gli Amministratori di Sistema che la Provincia di Cuneo.

## 9.12 ULTERIORI NORME E MISURE DI SICUREZZA

1. La sicurezza del sistema informativo provinciale è soggetta a costante evoluzione dovuta al continuo mutare delle minacce informatiche, che comporta l'adozione di contromisure sempre differenti e specifiche al verificarsi di attacchi o eventi particolari. A tal fine, i Sistemi Informativi adottano le misure di sicurezza che si rendono necessarie per la tutela del sistema informativo provinciale ed informano gli utenti tramite messaggi di posta elettronica, informative o circolari pubblicate nella intranet e/o tramite altri canali circa le ulteriori norme e misure di sicurezza da osservare.

## Art. 10. DISPOSIZIONI RIGUARDANTI LA REVOCA DELL'ASSEGNAZIONE DELLE DOTAZIONI E DELL'ACCESSO AL SISTEMA INFORMATIVO PROVINCIALE

1. Alla conclusione del rapporto di lavoro o allo scadere del rapporto di collaborazione cessano l'assegnazione delle Dotazioni informatiche e l'accesso al sistema informativo provinciale.
2. I dispositivi mobili (ad es. cellulari, tablet, PC portatile) assegnati agli utenti devono essere contestualmente riconsegnati ai Sistemi informativi.
3. Le abilitazioni dell'utente di cui al punto 5.1 vengono disattivate con riferimento:
   a) alla data di cessazione resa evidente dal settore Personale per i dipendenti (5.1.a) o dalla Segreteria Generale per i titolari di cariche politiche (5.1.b);
   b) alla data indicata nella richiesta di abilitazione per gli utenti di cui al precedente punto 5.1.c;
   c) su richiesta motivata del Segretario Generale o del Dirigente.
4. Quando il rapporto di lavoro o di collaborazione venga a cessare, è fatto divieto all'utente di conservare, duplicare, comunicare o diffondere informazioni e dati, personali o meno, di cui si è venuti a conoscenza per esigenze professionali.
5. In qualunque momento è facoltà del Segretario Generale o dei Dirigenti di disporre la revoca temporanea o definitiva dell'assegnazione dei dispositivi di telefonia mobile, tablet o PC portatili assegnati ai dipendenti.

## Art. 11. ASSISTENZA INFORMATICA

1. Gli Amministratori di Sistema forniscono l'assistenza informatica agli utenti del sistema informativo provinciale dal lunedì al venerdì dalle ore 9 alle ore 12 e, nei pomeriggi del lunedì, martedì e giovedì, dalle ore 14:30 alle 16:30.
2. L'assistenza informatica viene erogata previa richiesta all'indirizzo di posta elettronica assistenza.informatica@provincia.cuneo.it o al numero di telefono dedicato indicato nella intranet provinciale.
3. Nella richiesta di assistenza trasmessa via posta elettronica indicare sempre:
   a) il nominativo del chiamante, possibilmente con il recapito telefonico;
   b) descrivere sinteticamente la natura del problema;
   c) nel caso sia necessario l'intervento in loco, indicare l'ubicazione dell'ufficio;
4. Gli Amministratori di Sistema intervengono sulle postazioni utente, in presenza dell'utente o concordando l'intervento in assenza, su richiesta dell'utente stesso. Nei casi in cui sia sufficiente l'intervento da remoto, sarà fatto su richiesta dell'utente e con software che evidenzi che un Amministratore di Sistema è collegato da postazione remota.

## Art. 12. DISPOSIZIONI IN MERITO AI CONTROLLI

1. La Provincia di Cuneo, attraverso i propri Amministratori di Sistema, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione del sistema informativo provinciale, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono

stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali. In caso di uso di dispositivi elettronici personali, trova applicazione l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82.

2. Nelle more dell'adozione delle Linee guida per lo svolgimento degli accertamenti da parte dell'Agenzia per l'Italia Digitale, dovendo garantire la sicurezza e la protezione del sistema informativo, la Provincia si riserva la facoltà di effettuare, attraverso gli Amministratori di Sistema, controlli saltuari e occasionali sulle Dotazioni informatiche, garantendo agli utenti il rispetto dei principi di liceità, pertinenza e non eccedenza previsti dalla normativa applicabile, di quanto previsto dai provvedimenti del Garante della Privacy, nonché il rispetto del divieto dei controlli a distanza dei lavoratori dipendenti.
3. La Provincia si riserva, in particolare, di monitorare il sistema informativo provinciale e le Dotazioni informatiche nei seguenti casi:
   a) necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
   b) constatazione di utilizzo indebito della posta elettronica e della rete Internet;
   c) necessità di effettuare verifiche tese alla protezione del patrimonio della Provincia;
   d) presenza di casi di abusi da parte di singoli utenti;
   e) presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.
4. Le modalità con cui verranno effettuati i controlli saranno le seguenti:
   a) i controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di utenti, su dati aggregati ed anonimi tramite l'analisi di statistiche generali;
   b) successivamente, verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o in presenza di anomalie reiterate;
   c) in ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori.
4. I controlli potranno anche essere effettuati in ottemperanza alla richiesta dell'Autorità Giudiziaria o della Polizia giudiziaria.

## Art. 13. BACKUP E CONSERVAZIONE DEI DATI

1. Quotidianamente ed in modo automatico vengono effettuati i backup delle cartelle di servizio e personali del file server e dei server virtuali presenti nel cloud, completi dei software aziendali centralizzati ivi installati, e del database centralizzato installato nel cloud ed utilizzato da detti software. I backup giornalieri sono conservati per un massimo di:
   a) 3 mesi nel caso del file server contenente le cartelle di servizio e personali con queste caratteristiche:
      - salvataggio quotidiano mantenimento 21 giorni
      - salvataggio settimanale mantenimento 3 mesi
   b) 14 giorni nel caso dei server virtuali e dei software aziendali ivi installati;
   c) 15 giorni nel caso del database centralizzato con queste caratteristiche:
      - salvataggio settimanale mantenimento 3 mesi
      - salvataggio mensile mantenimento 12 mesi
      - salvataggio annuale mantenimento 3 anni;
2. Il backup dei dati presenti nei server fisici e virtuali e dei software aziendali ivi installati, situati presso la Sede della Provincia e non migrati nel cloud per ragioni tecniche, sono conservati per un massimo di 30 giorni.
3. I dati contenuti nei backup possono essere trattati dagli Amministratori di Sistema nelle seguenti ipotesi:

a) nel caso in cui sia necessario un intervento volto al recupero di dati;
b) per esigenze di diagnostica di malfunzionamenti e/o di manutenzione del sistema informativo provinciale;
c) per corrispondere ad eventuali richieste della Polizia giudiziaria e/o dell'Autorità giudiziaria;

4. L'Amministratore di Sistema può, in qualunque momento, procedere alla rimozione di ogni file o software che riterrà essere pericoloso per la sicurezza del sistema informativo provinciale, informando successivamente il Dirigente dei Sistemi Informativi ed il dipendente interessato dell'operazione effettuata.
5. Il contenuto delle cartelle di servizio e delle cartelle personali presenti nei file server saranno conservati senza limiti di tempo e non saranno cancellati dagli Amministratori di Rete, fatta salva la casistica di cui al punto precedente.
6. I settori e gli uffici detentori dei dati, personali o meno, dovranno provvedere autonomamente alla cancellazione in funzione del tipo di trattamento di dato effettuato e della durata di conservazione necessaria per lo svolgimento dei compiti istituzionali o richiesta dalla normativa.
7. Fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano la Provincia a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), trascorsi 30 giorni dalla cessazione del rapporto di lavoro dei dipendenti, tutti i dati salvati nella casella di posta elettronica personale e nella cartella personale nel file server saranno cancellati dagli Amministratori di Sistema.
8. Fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano la Provincia stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), il log del traffico internet a siti vietati è conservato per un massimo di 3 mesi ed è automaticamente cancellato dal sistema.

## Art. 14. REVISIONE PERIODICA DEL REGOLAMENTO

1. Il presente Regolamento è aggiornato periodicamente in considerazione di modifiche, innovazioni, eventi o esigenze rilevanti per le finalità del Regolamento relativamente a:
   - modifiche organizzative dell'Ente;
   - modifiche e/o innovazioni di carattere normativo o giurisprudenziale;
   - emanazione di Linee guida da parte dell'Agenzia per l'Italia Digitale;
   - modifiche e/o innovazioni di carattere tecnico o informatico;
   - esperienze maturate, nel periodo di riferimento, in applicazione del Regolamento che richiedano modifiche al testo adottato;
   - nuove esigenze di sicurezza.

## Art. 15. PUBBLICITÀ

1. Il presente Regolamento è pubblicato nella intranet dell'ente in intranet.provincia.cuneo.it e sul portale internet provinciale in www.provincia.cuneo.it.

## Art. 16. OSSERVANZA DEL REGOLAMENTO

2. Il mancato rispetto o la violazione delle regole contenute nel Regolamento è perseguibile con provvedimenti disciplinari previsti dal C.C.N.L. e, qualora si verifichino gli estremi per la sussistenza della responsabilità civile o penale, altresì con le azioni civili e penali previste dalle leggi vigenti.
3. L'inosservanza delle norme comportamentali descritte nel presente Regolamento da parte degli utenti può altresì comportare il risarcimento di eventuali danni arrecati alle Dotazioni in uso.