REGIONE CAMPANIA

UFFICIO SPECIALE

PER LA CRESCITA E LA TRANSIZIONE DIGITALE

DISCIPLINARE INTERNO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Aggiornamenti e Revisioni		
Revisione n.	**Oggetto**	**Data**
01	Prima Stesura	24/11/2023

	Struttura	Nome	Data
Redatto da:	Regione Campania	IT Asset Manager Manuela Serrao	20/11/2023
Verificato da:	Regione Campania	Responsabile SGI Maria Di Sarno	21/11/2023
Approvato da:	Regione Campania	Responsabile dell'US 11 Massimo Bisogno	22/11/2023
Emesso da:	Regione Campania	Ufficio Speciale per la Crescita e la Transizione Digitale	24/11/2023

INDICE

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete Internet dai PC fissi e portatili e dai dispositivi mobili, espone l'Amministrazione regionale, i dipendenti, i collaboratori nonché gli utenti dei servizi offerti dall'Ente, a rischi derivanti dalla perdita totale o parziale della riservatezza, integrità e disponibilità del Sistema Informatico e dei dati in esso contenuti.
Pertanto, al fine di mitigare tali rischi in relazione a eventuali comportamenti non idonei attuati da parte degli utilizzatori delle risorse informatiche, che potrebbero comportare danni, anche patrimoniali o d'immagine, nonché sanzioni derivanti da violazioni di specifiche disposizioni di legge, l'Ente ha deciso di adottare un Regolamento interno.
Tale Regolamento è redatto in conformità alle Policy di Sicurezza delle Informazioni, in armonia con il Codice di Comportamento della Regione Campania e in ottemperanza al principio di responsabilizzazione del Titolare del Trattamento di dati personali enunciato dal Regolamento UE n. 2016/679 (di seguito anche GDPR). Le regole contenute nel presente Regolamento, si aggiungono ed integrano le specifiche istruzioni fornite al personale da parte del Responsabile dell'Ufficio Speciale per la crescita e la transizione al digitale, in attuazione della normativa vigente per il trattamento dei dati personali, e completano le informazioni già fornite ai suddetti interessati in ordine alle modalità con cui potranno effettuarsi i necessari controlli o ai provvedimenti disciplinari conseguenti alle violazioni.

TITOLO I: INTRODUZIONE

Art. 1 Oggetto del documento

Le disposizioni del presente Regolamento disciplinano l'uso delle risorse informatiche della Regione Campania, così come definite al successivo art. 3.
Le risorse informatiche sono messe a disposizione degli utenti, definiti al successivo art. 2, comma 1, allo scopo di perseguire le finalità istituzionali dell'Amministrazione.
L'Ente promuove ogni opportuna misura, organizzativa, fisica e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà di Regione Campania e disciplina le modalità con cui effettuerà i relativi controlli.
Gli utilizzatori delle risorse informatiche sono tenuti a contattare il Responsabile della Sicurezza prima di intraprendere qualsiasi attività non esplicitamente ricompresa nelle disposizioni del presente Disciplinare, al fine di garantire che tali attività non siano in contrasto con le politiche di sicurezza informatica stabilite dall'Ente.

Art. 2 Ambito di applicazione

Il presente Regolamento si applica a tutti gli utilizzatori delle risorse informatiche di Regione Campania, così come individuati all'art. 3. senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori della Regione Campania a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).
Il presente Regolamento viene pubblicato anche sul sito istituzionale della Regione Campania, nell'apposita sezione "Amministrazione trasparente» Disposizioni generali / Atti generali / Ufficio per la Crescita e la Transizione Digitale".
La Regione Campania, contestualmente alla sottoscrizione del contratto di lavoro o all'atto di conferimento dell'incarico, consegna e fa sottoscrivere ai nuovi assunti, con rapporti comunque denominati, copia del presente Regolamento.

Art. 3 Definizioni

Ai fini dell'applicazione del presente Regolamento deve intendersi:
Amministratore del sistema: la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché alla protezione dei dati, quali l'amministratore di basi di dati, l'amministratore di reti e di apparati di sicurezza e l'amministratore di sistemi software complessi
Archivio di rete: le cartelle condivise nella rete locale o sui cloud di Regione Campania per la memorizzazione di informazioni in formato digitale a scopo esclusivamente lavorativo.
Cartelle di lavoro dell'Operatore: la cartellain cui sono memorizzati i documenti informatici relativi all'attività dell'Operatore.
Casella di posta elettronica personale: la casella di posta elettronica istituzionale assegnata agli Operatori di Regione Campania.
Casella di posta elettronica di servizio: la casella di posta elettronica istituzionale assegnata alle strutture o ai servizi.
Casella di posta elettronica certificata: la casella di posta elettronica certificata della struttura o del servizio.
CIE: Carta d'identità elettronica - è un documento di identità e garantisce il riconoscimento fisico in ogni caso di richiesta di identificazione.
Comunicazioni esterne: le comunicazioni esterne al dominio di posta elettronica della Regione Campania.
Credenziali riconosciute: credenziali telematiche riconosciute dall'Ente e utilizzate per l'accesso alle risorse informatiche
Dati personali: dati personali ai sensi del GDPR.
Dispositivi mobili: qualsiasi dispositivo elettronico utilizzabile seguendo la mobilità dell'utente quali, a titolo esemplificativo e non esaustivo, telefoni cellulari, palmari, smartphone, tablet, laptop, ecc.
ICT: Information and Communication Technology
Messaggio di posta elettronica: messaggio inviato/ricevuto da una casella di posta elettronica personale/di servizio o attraverso un applicativo che utilizza un server di posta elettronica.

Operatore: il dipendente e il collaboratore (lavoratore parasubordinati, lavoratore somministrato, lavoratore in stage, ecc.) espressamente autorizzato ad accedere ed utilizzare i sistemi informatici della Regione Campania.
PEC: è un sistema di comunicazione quale basato sulla posta elettronica ordinaria, a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere ai messaggi un valore legale equiparato alla Posta Raccomandata con ricevuta di ritorno (A/R). Il valore legale è assicurato dai gestori del servizio PEC del mittente e del destinatario, per le sole comunicazioni inviate da una casella PEC e ricevute da un'altra casella PEC, che certificano: · data e ora dell'invio del messaggio da parte del mittente; · data e ora dell'avvenuta consegna del messaggio al destinatario; · integrità del messaggio (ed eventuali allegati) nella trasmissione da mittente a destinatario. Le caselle PEC dell'Ente sono, di norma, integrate nel sistema di protocollo informatico.
Profilo operatore: insieme di azioni che un operatore può effettuare su un dataset di dati in ragione del rapporto con l'Ente.
Rete telematica dell'Ente, nel seguito semplicemente la Rete, l'infrastruttura fisica e logica che permette l'interconnessione degli apparati dell'Ente, per la trasmissione dati fra loro e con la rete Internet.
Sistema informatico della Regione Campania: l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, personal computer, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Ente.
Smartphone: il dispositivo portatile che abbina funzionalità di gestione di dati personali e di telefono.
Social: servizi web (social network, newsletter, mailing list, forum, instant messaging, wiki, etc.) utilizzati per creare e mantenere reti virtuali e comunità on-line costituite da gruppi di persone che si relazionano tra loro da un qualsiasi tipo di legame (amicizia, di interessi, lavorativo, etc.). L'Ente può utilizzare i social per comunicare con target di utenti spesso non raggiungibili con i servizi tradizionali, informare e far partecipare i cittadini alla vita istituzionale dell'Ente nonché per dialogare con le altre amministrazioni pubbliche.
Rischio Informatico: è la probabilità che minacce di natura accidentale o dolosa, sfruttino le vulnerabilità intrinseche di una risorsa informatica e quindi causare danni di varia natura (economici, reputazionali, ecc.) ad un'Organizzazione. **SPID:** Sistema Pubblico d'Identità Digitale. Rappresenta, tramite un'unica credenziale, l'identità digitale e personale di ogni cittadino, con cui è riconosciuto dalla Pubblica Amministrazione per utilizzare in maniera personalizzata e sicura i servizi digitali messi a disposizione dalle amministrazioni centrali e locali.
Utente: il soggetto pubblico e privato esterno all'Ente e diverso dall'Operatore, espressamente autorizzato ad accedere e utilizzare i sistemi informatici e telematici dell'Ente.
Wi-Fi: è una tecnologia di reti wireless che consente a dispositivi come computer fissi, dispositivi mobili e altre apparecchiature (es. stampanti e videocamere) di interfacciarsi con Internet.

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni rientranti nel patrimonio dell'Ente e sono da considerarsi di sua esclusiva proprietà. Il loro utilizzo è consentito solo per adempiere alle mansioni lavorative affidate a ciascun operatore/utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti all'attività svolta per l'ente, e comunque per l'esclusivo perseguimento dei fini istituzionali.

TITOLO II: NORME PER L'ACCESSO AL SISTEMA INFORMATICO

Gli Operatori e Utenti possono accedere alle risorse informatiche esclusivamente per lo svolgimento delle mansioni lavorative/incarichi ad essi affidati, in forza di un contratto o altro accordo in essere con Regione Campania, ed esclusivamente per scopi leciti.
Gli Operatori e Utenti possono accedere al Sistema Informatico solo previa autorizzazione del Responsabile del Sistema Informatico, tramite credenziali di autenticazione (es. username e password) o altri metodi di autenticazione "forte", quali la Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE) e SPID.
Gli Operatori e gli eventuali Utenti non possono cedere a soggetti terzi, le loro credenziali di accesso al Sistema informatico dell'Ente
Gli Operatori e gli Utenti possono, laddove previsto, accedere al Sistema informatico, anche tramite la rete wi-fi dedicata, mediante le credenziali loro assegnate dal Responsabile del Sistema Informatico o persone da lui delegate, utilizzando i PC in dotazione dell'Ente appositamente predisposti ovvero utilizzando proprie attrezzature preventivamente autorizzate dal Responsabile del Sistema Informatico. Gli Operatori e gli Utenti si impegnano ad evitare pratiche che possono esporre l'Ente a rischi informatici (es. possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche di proprietà dell'Ente). Laddove tali pratiche non siano evitabili, gli Operatori e gli Utenti si impegnano ad adottare comportamenti tesi a minimizzare tali rischi.
Gli Operatori e gli Utenti sono tenuti a segnalare presunte o accertate violazioni alla sicurezza delle risorse informatiche dell'Ente, al Responsabile del Sistema Informatico o persona da lui delegata e per conoscenza al Responsabile della Sicurezza delle Informazioni e al Responsabile dell'Ufficio.
Gli strumenti adottati per l'accesso Sistema informatico dell'Ente, sono di uso strettamente personale e pertanto l'Operatore o gli Utenti sono tenuti a custodirli in modo appropriato, al fine di garantirne la riservatezza e l'integrità.
La Regione Campania si riserva di applicare specifiche clausole contrattuali o adottare accordi di riservatezza con gli Operatori e Utenti del Sistema Informatico, per garantire la riservatezza e la non-divulgazione delle informazioni critiche dell'Ente, secondo quanto previsto dalle normative vigenti. Tali accordi, devono necessariamente contemplare tutti i requisiti necessari ad assicurare la protezione del Sistema Informatico dell'Ente.

Art. 4 Attribuzione e gestione delle credenziali e dei profili di accesso

Le credenziali di autenticazione per l'accesso al Personal Computer vengono assegnate dall'Ufficio Speciale per la crescita e la transizione digitale, previa formale richiesta del Dirigente del Settore nel caso di nuovo utente.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'Ufficio Speciale per la crescita e la transizione digitale, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

- La parola chiave dovrà essere formata come minimo da otto caratteri appartenenti ad almeno tre dei seguenti gruppi:Lettere minuscole (a-z);
- Lettere maiuscole [A-Z];
- Numeri [0-9];
- Caratteri speciali [es. #, &, !, -, ecc.);

e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

Decorso il termine di cui al punto precedente senza che l'utente abbia modificato la propria parola chiave, le credenziali di autenticazione saranno disabilitate. Per riabilitarle sarà necessario procedere d'intesa con l'Ufficio Speciale per la crescita e la transizione digitale.

Nessuno è autorizzato a richiedere ad un Operatore o ad un eventuale Utente la propria username e password ed ognuno di questi deve mantenere segrete le proprie credenziali di accesso.

Nell'utilizzo del Sistema informatico ogni Operatore o Utente è identificato univocamente dalle proprie credenziali, che vengono tracciate dai vari servizi informatici.

L'Operatore e l'eventuale Utente sono considerati gli unici responsabili dell'attività espletata tramite la propria username, la propria CNS, la propria CIE e le proprie credenziali SPID; vige a tal fine una presunzione di corrispondenza tra l'Operatore/Utente e username e, laddove applicabile, la CNS, la CIE o SPID.

In linea con quanto previsto dalla politiche di sicurezza dell'Ente, al fine di ridurre le opportunità di modifica o di uso improprio e/o non autorizzato al Sistema Informatico, sono avviate da parte del Responsabile della sicurezza informatica, delle verifiche periodiche in merito alla sussistenza delle condizioni per il mantenimento delle credenziali di autenticazione (utenze) e dei profili autorizzativi per l'accesso al Sistema informatico dell'Ente, con particolare attenzione ai profili autorizzativi privilegiati (es. Amministratori del sistema).

Inoltre, al fine di aggiungere un livello di protezione al processo di accesso, per tutti gli account è attivo il servizio di autenticazione a Fattori Multipli (MFA - Multi factor Authentication).

Art. 5 Sospensione delle credenziali

La sospensione delle credenziali di autenticazione viene effettuata dal Responsabile della sicurezza informatica ogni qualvolta, in caso di rischio di accessi illeciti o di compromissione della password, sia necessario per garantire la sicurezza del Sistema informatico dell'Ente, nonché in relazione a quanto previsto all'Art. 36 (Sanzioni) del presente Regolamento.
La revoca della sospensione delle credenziali viene effettuata dal Responsabile della sicurezza informatica su richiesta del Responsabile dell'Ufficio/Settore ove opera l'operatore/utente.

Art. 6 Disattivazione delle credenziali

La disattivazione delle credenziali di autenticazione non utilizzate da almeno 90 giorni, viene garantita dal Responsabile della sicurezza informatica attraverso un meccanismo automatico.
Il Responsabile della sicurezza informatica, al momento della cessazione del rapporto di lavoro di un dipendente o di un collaboratore, comunicata dalla Direzione Risorse Umane, disattiva tempestivamente tutte le utenze associate allo stesso.
Il Responsabile dell'Ufficio richiede al Responsabile della sicurezza informatica, la disattivazione delle credenziali per tutte le altre categorie di Operatori non regolamentate al comma 2 del presente articolo. Il Responsabile della sicurezza informatica disattiverà tempestivamente tutte le utenze associate.
L'Ufficio Speciale per la Crescita e la transizione digitale provvede a disabilitare le credenziali utente associate agli Utenti dell'Amministrazione, nel momento in cui non sussistano più le condizioni per il mantenimento delle credenziali utente e/o dei relativi profili autorizzativi (es. cambio di ruolo o mutamento delle mansioni svolte dal titolare dell'utenza, dimissioni).
Prima della disattivazione della casella di posta elettronica associata ai soggetti di cui al comma 2 del presente articolo, sarà possibile concordare con il Responsabile della sicurezza informatica l'eventuale invio di un messaggio di posta elettronica automatico, valido per un periodo di 30 giorni a partire dalla cessazione del rapporto di lavoro, che indichi altresì, un eventuale indirizzo di posta elettronica istituzionale alternativo, cui inviare i messaggi attinenti all'attività svolta, fermo restando la sospensione immediata di qualunque procedura

atta a consentire la consultazione, da parte dei suddetti soggetti, del contenuto dei messaggi già pervenuti o che potrebbero pervenire.
Decorsi 60 giorni dalla cessazione dal rapporto di lavoro di un Operatore, il Responsabile della sicurezza informatica provvederà alla disattivazione della casella di posta elettronica personale dello stesso.
I contenuti della casella di posta elettronica vengono conservati sui server dell'Ente per un anno dalla cessazione del rapporto di lavoro per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti posti dall'art. 160-bis, del Codice privacy, in base al quale "La validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali".
In relazione agli scopi perseguiti, la struttura interessata dovrà fornire elementi in ordine alle specifiche ragioni che rendano necessario aumentare i tempi di conservazione sui server.
Le disposizioni di cui ai precedenti commi si applicano anche al personale in quiescenza titolari di incarichi, ancorché gratuiti, con l'Amministrazione.

Art. 7 Accesso alla casella di posta elettronica personale e alla cartella di lavoro in caso di assenza del titolare

L'accesso alla casella di posta elettronica personale e alla cartella di lavoro in caso di assenza del titolare è possibile nell'eventualità e nelle modalità previste nei commi seguenti del presente articolo.
L'Operatore in caso di assenza preventivata dal servizio è tenuto ad attivare il servizio di risposta automatica, al fine di avvisare i mittenti, in caso di comunicazioni attinenti all'attività lavorativa, di contattare altra persona competente ovvero l'Ufficio competente.
In casi assolutamente eccezionali, ove vi sia la necessità di verificare il contenuto della cartella di lavoro e della posta elettronica personale del titolare, in assenza di quest'ultimo, il Responsabile dell'Ufficio e il Responsabile della sicurezza informatica avvieranno la procedura redigendo apposito verbale ed informando il lavoratore con tempestività e per iscritto, trasmettendogli altresì copia del verbale redatto. Per le attività di cui al punto precedente, a ciascun Operatore è preventivamente fornita un'apposita informativa in cui siano specificati i limiti e le modalità di accesso alla cartella di lavoro e alla posta elettronica istituzionale da parte del Responsabile dell'Ufficio e del Responsabile della sicurezza informatica.

Art. 8 Violazioni

La violazione di quanto previsto dal presente documento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dal CCNL.
Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o

addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici dell'Ente.
In caso di violazione accertata delle regole e degli obblighi esposti in questo documento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

TITOLO III: NORME PER L'UTILIZZO DELLE APPARECCHIATURE INFORMATICHE E TELEMATICHE

CAPO I: UTILIZZO PERSONAL COMPUTER

Art. 9 Personal Computer (PC)

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
Il personal computer dato in affidamento all'utente permette l'accesso alla rete della Regione Campania solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.
Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'Ufficio Speciale per la crescita e la transizione digitale né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa Regione Campania a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
Salvo preventiva espressa autorizzazione dell'Ufficio Speciale per la crescita e la transizione digitale, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem).
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale dell'Ufficio Speciale per la crescita e la transizione digitale nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di suo inutilizzo. Se si lascia incustodita la scrivania durante l'orario di lavoro, spegnere il Personal Computer o, se l'apparecchiatura deve restare accesa, bloccarne l'accesso mediante le apposite funzionalità che richiedono la ridigitazione della password per riaccedere (es. salvaschermo).

In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Art. 10 PC portatili e accessori temporaneamente assegnati

L'Operatore è responsabile del PC portatile e/o accessori (macchina fotografica, videoproiettore) a lui temporaneamente assegnati e deve custodirli con diligenza, sia all'interno degli uffici dell'Ente, sia durante gli spostamenti esterni, fino alla loro riconsegna.
Ai PC portatili dell'Ente si applicano le regole previste dal presente Regolamento anche al di fuori della Rete e degli Uffici dell'Amministrazione regionale.
Particolare attenzione deve essere prestata nell'utilizzo e nella custodia del PC portatile al di fuori della Rete e degli uffici dell'Ente, nella connessione a reti telematiche esterne e nella cancellazione sicura di eventuali file e dati personali memorizzati nel medesimo, prima della riconsegna.
Tali disposizioni si applicano anche nei confronti di incaricati esterni.

Art. 11 Supporti e dispositivi informatici di memorizzazione

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
I dati personali ai sensi del GDPR trattati nell'ambito dell'attività lavorativa possono essere replicati su supporti e dispositivi informatici di memorizzazione (dischi locali dei PC, memorie esterne), banche dati e documenti, solo previa ed esplicita autorizzazione del Responsabile dell'Ufficio di appartenenza in attuazione delle misure di sicurezza adottate dall'Ente.
Gli Operatori devono provvedere periodicamente (almeno ogni tre mesi) alla cancellazione dei file obsoleti, dai propri supporti e dispositivi informatici.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare l'Ufficio Speciale per la crescita e la transizione digitale e seguire le istruzioni da questo impartite.
In ogni caso, supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Art. 12 Dismissioni e riutilizzo di apparecchiature informatiche

In caso di dismissione o riutilizzo delle apparecchiature informatiche, ciascun utente dovrà contattare l'Ufficio Speciale per la crescita e la transizione digitale e seguire le istruzioni da questo impartite.
Prima della dismissione o riutilizzo, delle apparecchiature informatiche contenenti dati personali ai sensi del GDPR, l'Ufficio Speciale attuerà tutte le misure atte a garantire la cancellazione sicura di tali dati in linea con quanto previsto dalla normativa vigente.

Art. 13 Help desk e assistenza remota

Il personale incaricato dall'Ufficio Speciale per la crescita e la transizione digitale ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

CAPO II: UTILIZZO DEI CANALI DI COMUNICAZIONE

Art. 14 Principi generali

La posta elettronica è uno dei principali mezzi di comunicazione e di trasmissione di documenti, informazioni e dati dell'Ente.
Esso costituisce il recapito elettronico istituzionale del titolare, destinato al conseguimento dei fini istituzionali dell'Ente.
Il servizio di posta elettronica è operante con continuità 24 ore al giorno per 365 giorni l'anno.
L'Ufficio speciale per la crescita e la transizione digitale fornisce a tutte le strutture in cui è articolata l'organizzazione regionale una casella di posta elettronica PEO e una casella di posta elettronica certificata PEC.
Fornisce, inoltre, a tutti i propri dipendenti una casella di posta elettronica PEO (casella personale) per soli fini istituzionali.
L'Ufficio può fornire una casella di posta elettronica ai propri collaboratori, previa richiesta del Dirigente della struttura di afferenza: la peo assegnata ai collaboratori porterà al proprio interno la dicitura "guest" (ad esempio mario.rossi@guest.regione.campania.it) permettendo così di individuare il mittente come un collaboratore non come un utente/dipendente di Regione Campania;
Gli utenti hanno l'obbligo di procedere alla tempestiva lettura della corrispondenza pervenuta nella propria casella, almeno una volta al giorno.

Art. 15 Gestione del Servizio di posta elettronica

Il servizio di posta elettronica ordinaria e quello di posta elettronica certificata sono erogati in cloud da uno o più fornitori di servizi, cui è assegnata la responsabilità del suo corretto funzionamento. In particolare, i fornitori sono tenuti a:

1. adottare le misure più idonee a garantire la continuità, la disponibilità e la sicurezza del servizio;
2. gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali;
3. informare tempestivamente gli utenti, con un anticipo almeno di 24 ore, di eventuali interruzioni del servizio che si rendessero necessarie per cause di forza maggiore;
4. monitorare i livelli di servizio del sistema al fine di garantirne la massima efficienza;
5. monitorare l'utilizzo del servizio da parte degli utenti al fine di evidenziarne usi scorretti o non consentiti;
6. offrire assistenza tecnica agli utenti.

I fornitori di servizi non effettuano alcuna visura, controllo, censura, modifica, cancellazione dei messaggi di posta elettronica ricevuti e inviati dagli utenti, a meno che ciò non venga richiesto dalla legge ovvero nel caso in cui ciò si renda necessario per adempiere ad una disposizione di legge, ad un ordine giudiziario o governativo.
Nel caso di messaggi ritenuti dannosi dagli algoritmi automatici di gestione dei servizi di posta elettronica, gli stessi vengono posti in "quarantena" e l'utente viene avvisato di tale circostanza.

Art. 16 Gestione delle caselle di posta elettronica

L'Ufficio Speciale per la Crescita e la Transizione Digitale provvede:

1. ad attivare automaticamente per ogni dipendente, conseguentemente alla sua assunzione in servizio, una casella di posta elettronica ordinaria;
2. a disattivare automaticamente per ogni dipendente, conseguentemente alla sua cessazione dal servizio, la relativa casella di posta elettronica;
3. a mantenere attiva, previa richiesta del Dirigente della struttura di afferenza, la casella di posta dei dipendenti in quiescenza per ragioni legate al servizio prestato;
4. ad attivare/disattivare caselle di posta elettronica per gli Amministratori a seguito di comunicazione della Segreteria di Giunta;
5. ad attivare/disattivare caselle di posta elettronica per i collaboratori, previa richiesta del Dirigente della struttura di afferenza;
6. ad attivare/disattivare le caselle di posta elettronica di struttura a seguito di ogni modifica organizzativa dell'Ente.

L'attivazione di una casella di posta elettronica è effettuata attraverso l'assegnazione di un codice identificativo dell'utente (*user id*), la relativa parola chiave riservata (*password*) iniziale ed un indirizzo.

Gli indirizzi di posta elettronica per le caselle personali hanno la seguente nomenclatura, salvo casi di omonimia od esigenze particolari:
<nome utente>.<cognome utente>@regione.campania.it
Esempio: carlo.rossi@regione.campania.it
Nel caso di doppio nome o doppio cognome vengono riportati entrambi, senza spazio o punteggiatura di separazione.
Gli indirizzi di posta elettronica per le caselle di struttura hanno la seguente nomenclatura:

1. Per le Direzioni Generali:
   <dg><numero direzione>@regione.campania.it
   Esempio: us11@regione.campania.it
2. Per le Unità Organizzative Dirigenziali:
   <uod><codice tipologia><codice direzione><numero uod>@regione.campania.it
   Esempio: uod601101@regione.campania.it o US11.uod01@regione.campania.it
   Per le Unità Organizzative Dirigenziali di staff:
   <staff><codice tipologia><codice direzione><numero uod>@regione.campania.it
   Esempio: staff601191@regione.campania.it

Art. 17 Caselle di posta elettronica certificata (PEC)

La casella di Posta Elettronica Certificata (PEC) istituzionale della Giunta della Regione Campania per la corrispondenza, sia in ingresso sia in uscita, è inserita sia nell'indice delle Pubbliche Amministrazioni (IPA) che sul sito istituzionale di Regione Campania nella sezione "Amministrazione Trasparente".
A tale casella in casi di necessità possono far riferimento tutti i cittadini, le imprese e gli Enti dopo che abbiano prodotto regolare istanza mediante il portale regionale.
La Giunta della Regione Campania fornisce inoltre, a tutte le strutture apicali in cui è articolata la propria organizzazione, una unica casella di Posta Elettronica Certificata (caselle PEC di struttura) per la comunicazione con tutti quei soggetti esterni muniti di PEC con cui la struttura intrattiene rapporti istituzionali.
Ulteriori caselle PEC potranno essere assegnate dall'Ufficio Speciale per la Crescita e la Transizione Digitale, o su richiesta delle strutture, solo laddove finalizzate a specifiche applicazioni, quali comunicazioni automatiche da/verso sistemi automatizzati.
L'Ufficio Speciale per la Crescita e la Transizione Digitale cura l'assegnazione delle caselle PEC di struttura, chiedendo ai responsabili di struttura una volta generata di provvedere alla loro attivazione, mediante sottomissione del link ricevuto nella prima e-mail e generazione della relativa password.
Per ogni casella PEC di struttura, è individuato il soggetto Utilizzatore (Dirigente della struttura o suo delegato), cui sono fornite le credenziali di accesso per l'utilizzo.
Le caselle PEC sono utilizzabili per scambiare mail certificate con qualunque titolare di PEC.

L'Ufficio Speciale per la Crescita e la Transizione Digitale ha cura della gestione e aggiornamento dell'elenco di tutti gli indirizzi di posta elettronica certificata, regolarmente pubblicati sul sito IPA, Indice delle Pubbliche Amministrazioni.
Le regola di nomenclatura per le caselle di posta certificata seguono le regole di cui all'art. 4 del presente disciplinare e hanno il seguente dominio @pec.regione.campania.it.

Art. 18 Compiti e responsabilità

Il dipendente è responsabile della propria casella di posta elettronica personale.
Il collaboratore è responsabile della casella di posta elettronica assegnatagli.
Il Dirigente, o responsabile di struttura, è responsabile della casella di posta elettronica della struttura che dirige Il Dirigente, o responsabile di struttura, può delegare un dipendente alla gestione della casella di struttura. La delega va attribuita per iscritto.
L'utente è responsabile della segretezza del proprio userID e relativa password.
L'utente è responsabile del contenuto dei messaggi inviati dalla propria casella.
L'utente è responsabile di tutte le operazioni effettuate con la casella di posta elettronica relativa all'userID a lui associato.
L'utente è responsabile delle eventuali conseguenze pregiudizievoli che un uso improprio del servizio da parte del proprio userID potrebbero comportare a terze persone, e ciò in riferimento alla vigente normativa in materia civile e penale.
L'utente si impegna a comunicare all'Ufficio Speciale per la Crescita e la Transizione Digitale, non appena ne venisse a conoscenza, qualsiasi uso non autorizzato da parte di terze persone del proprio userID.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per la Regione Campania ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Dirigente del Settore.
È obbligatorio porre la massima attenzione nell'aprire i file allegati alla posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
Sarà comunque consentito al Dirigente del Settore ove opera l'utente, o a persona da questi formalmente individuata, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.
L'Ufficio Speciale per la crescita e la transizione digitale, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia

dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.

Al fine di ribadire agli interlocutori la natura esclusivamente professionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dalla Regione Campania potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate dal proprio regolamento.

Art. 19 Utilizzo posta elettronica -

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa

L'utente è tenuto ad attenersi alle seguenti prescrizioni nell'utilizzo del servizio di posta elettronica:

1. conformarsi alle indicazioni tecniche fornite dall'Ufficio Speciale per la Crescita e la Transizione Digitale;
2. non utilizzare la posta elettronica per trasmettere e diffondere materiali che non possono essere legalmente distribuiti per via telematica;
3. non usare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso;
4. non inviare e ricevere materiali e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
5. non utilizzare il servizio per inviare catene di lettere, solleciti commerciali, messaggi politici ovvero qualunque altro messaggio a persone che non abbiano acconsentito a tale procedura;
6. non utilizzare il servizio per motivi privati e/o per contatti interpersonali tra i dipendenti non inerenti all'uso d'ufficio;
7. non inviare messaggi ad una pluralità di destinatari (invii multipli) indiscriminatamente, eccedenti il numero dei reali interessati;
8. utilizzare con diligenza il servizio, evitando di sovraccaricare il sistema con l'invio di messaggi ed allegati di dimensioni inutilmente eccessive e/o contenenti inutili grafismi o d'immagini;
9. cancellare messaggi ricevuti inutili e di dimensioni eccessive;
10. utilizzare il servizio nel pieno rispetto del Codice di tutela dei dati personali;
11. adottare le necessarie cautele per assicurare la segretezza del proprio userID e della propria password; ove mai, sotto la sua personale responsabilità, le registri su un supporto qualsiasi, deve custodirle con la massima diligenza;
12. scegliere password non banali o comunque non contenenti riferimenti agevolmente riconducibili alla sua identità.

Le modalità operative per la fruizione del servizio dipendono dal sistema di posta elettronica adottato dall'Ente, e saranno rese pubbliche sul sito istituzionale della Regione Campania.

CAPO III: UTILIZZO DELLE RISORSE DI RETE

Art. 20 Collegamento alla rete locale

Per l'accesso alla rete della Regione Campania ciascun utente deve utilizzare esclusivamente Personal Computer, portatili e, più in generale, dispositivi autorizzati dall'Ufficio Speciale per la crescita e la transizione digitale.
È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
Le cartelle utenti presenti nei server della Regione Campania sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo e amministrazione da parte del personale individuato dall'Ufficio Speciale per la crescita e la transizione digitale. Si ricorda che tutti i dischi o altre unità di memorizzazione locali, nonché le aree di condivisione presenti sui server non sono soggette a salvataggio da parte dell'Ufficio Speciale per la crescita e la transizione digitale. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.
Le connessioni con modem o linee dirette, tra sistemi e la rete di Regione Campania, con reti e sistemi esterni, possono presentare un serio rischio per l'intera Amministrazione Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo della Regione Campania ed i dati in esso contenuti ciò può avvenire senza che il dipendente se ne renda conto. Per tale motivo, ogni collegamento dall'interno verso l'esterno e viceversa, deve essere approvato dall'Ufficio Speciale per la crescita e la transizione digitale.

Art. 21 Utilizzo di Internet

II PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
Non è consentito agli Operatori di:

- accedere ad Internet per motivi privati non inerenti al lavoro d'ufficio, fatte salve le operazioni consentite nel presente Disciplinare e con i limiti ivi indicati;
- effettuare il download o lo scambio peer-to-peer di materiale audiovisivo, fotografico, software ed in genere di ogni altra tipologia di materiale digitale non legati ad un uso d'ufficio e che possa sottintendere presunte o palesi violazioni del copyright in ambito nazionale ed internazionale.

Il Responsabile della sicurezza informatica produce periodicamente una statistica anonima dei siti web visitati dagli Operatori tramite la rete dell'Ente.
L'Operatore è considerato l'unico responsabile dell'attività espletata nella rete Intranet dell'Ente e nella Internet mediante le proprie credenziali di accesso e di autorizzazione.
Ogni Operatore è obbligato ad utilizzare il servizio di accesso al web, ponendo la massima attenzione alla sicurezza del Sistema informatico e telematico dell'Ente e nel rispetto di quanto previsto dal Codice di Comportamento Regionale e delle Policy di sicurezza dell'Ente.
Il Responsabile della sicurezza informatica potrà autorizzare la navigazione verso siti o categorie di siti bloccati, previa richiesta motivata, da parte del Responsabile dell'Area/Settore dell'Ufficio interessato, legata a specifiche ed inderogabili esigenze lavorative.

CAPO IV: ALTRI DISPOSITIVI

Art. 22 Stampanti, fotocopiatrici, scanner e fax

È cura dell'Operatore effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
Non è consentito stampare documenti o file molto lunghi o di contenuto grafico su stampanti comuni, se non strettamente necessario all'attività lavorativa.
Non è consentito stampare, fotocopiare o scansionare documenti personali su qualsivoglia stampante e/o fotocopiatrice.
È obbligatorio effettuare le stampe in modalità fronte-retro, fatta salva documentata impossibilità tecnica o amministrativa.
È fatto divieto agli Operatori effettuare la sostituzione del toner o di qualsiasi altra parte di ricambio sulle stampanti, sulle fotocopiatrici, sugli scanner. In caso di malfunzionamento delle apparecchiature in oggetto al presente articolo, gli Operatori sono tenuti a darne tempestiva comunicazione all'Ufficio Speciale per la crescita e la transizione al digitale.

Art. 23 Telefoni fissi

L'Operatore è responsabile dell'utilizzo del telefono fisso assegnato.
Il telefono fisso affidato all'Operatore dall'Ente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali mediante il telefono fisso a disposizione è consentito solo nel caso di comprovata necessità ed urgenza.

Art. 24 Telefoni cellulari e SIM

Si rinvia al "Disciplinare tecnico per l'assegnazione e l'utilizzo delle apparecchiature di telefonia mobile" - approvato con Decreto Dirigenziale n. 684 del 13/12/2022 della Direzione Generale per le risorse strumentali - nel quale sono indicate le policy di sicurezza

dall'assegnatario in attuazione del principio di responsabilizzazione (accountability) sancito dall'art. 24 Reg. (UE) 2016/679.

CAPO V: SMART CARD E FIRMA DIGITALE

Art. 25 Definizione dei ruoli per la gestione del certificato di firma digitale

Ai fini dell'assegnazione del certificato di firma digitale Il Responsabile dell'Ufficio/Struttura o un suo delegato autorizzato richiede il certificato a favore del titolare.
L'Ufficio speciale per la crescita e la transizione digitale provvede a fornire informazioni per ciò che attiene al ruolo e alle funzioni istituzionali dei dipendenti ai quali possono essere assegnati i certificati di firma digitale e individua e nomina gli incaricati del servizio; ai sensi dell'art. 36, comma 1 let. c) del CAD, autorizza il rilascio del certificato e ha inoltre la facoltà di richiedere la sospensione o la revoca del certificato.
Sono nominati dal Direttore Generale e responsabili su delega del Certificatore, i soggetti incaricati del servizio di firma digitale, dell'identificazione dei richiedenti, dell'attivazione delle procedure di emissione, revoca o sospensione dei certificati.
L'Incaricato del servizio di firma digitale trasmette al Responsabile dell'USCTD e/o suo delegato, l'elenco debitamente sottoscritto, delle persone richiedenti il certificato di firma digitale al fine del rilascio della relativa autorizzazione.
L'incaricato, ricevuta la richiesta di attivazione, convoca il richiedente per lo svolgimento delle operazioni di registrazione. Il richiedente deve presentarsi dall'Incaricato, nel giorno comunicatogli, munito di un valido documento di identità e del codice fiscale.

Art. 26 Compiti e responsabilità degli incaricati del servizio di firma digitale

Gli incaricati del servizio di firma provvedono a:

a. verificare con certezza l'identità del titolare.
b. rilasciare i certificati qualificati attraverso l'utilizzo dell'apposito Sistema informatico fornito dal Certificatore, seguendo le istruzioni operative previste dal Manuale Operativo del Certificatore.
c. informare il titolare riguardo agli obblighi assunti in merito alla protezione della segretezza delle chiavi private e al trattamento dei dati personali
d. supportare il titolare nelle ipotesi di revoca, sospensione o annullamento della sospensione delle firme attivate.
e. raccogliere le comunicazioni di rilascio/rinnovo, sospensione e/o revoca e conservarle con modalità sicure. individuare mensilmente i certificati la cui data di scadenza è compresa entro i trenta giorni solari successivi e, verificato il permanere delle condizioni per il rilascio, richiedere l'autorizzazione formale per il rinnovo degli stessi secondo quanto indicato al presente articolo, comma 1, let. c).
f. rispettare le misure di sicurezza previste nel presente disciplinare.
g. rispettare le necessarie procedure di sicurezza nell'esercizio delle proprie funzioni.

Art. 27 Obblighi del titolare del certificato di firma digitale

Il titolare del certificato di firma digitale è tenuto a:

a. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma, che utilizzerà personalmente e per ragioni istituzionali.
b. conservare con la massima diligenza e riservatezza i propri codici personali al fine di evitarne l'uso fraudolento da parte di terzi.
c. comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione all'incaricato del servizio di firma digitale ed informarlo dell'eventuale variazione del rapporto contrattuale con l'Ente regionale e di tutti i dati richiesti per l'emissione del certificato.
d. informare anticipatamente gli incaricati del servizio di firma digitale di ogni circostanza che renda necessaria o, comunque, opportuna la revoca o la sospensione del certificato e del dispositivo di firma a lui assegnato; deve altresì informare tempestivamente il suddetto incaricato di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

Art. 28 Causa di revoca e sospensione del certificato di firma digitale

La revoca di un certificato di firma digitale determina la cessazione anticipata della sua validità.
La revoca ha luogo su iniziativa di Certificatore, del Titolare, del Direttore Generale che ne ha autorizzato il rilascio.
A titolo esemplificativo e non esaustivo, interverrà la revoca nelle seguenti circostanze:

- cessazione del rapporto di lavoro del dipendente per qualsiasi causa
- perdita del ruolo, qualifica o funzione istituzionale che motivano l'assegnazione del certificato;
- smarrimento, furto o cambio del dispositivo di firma
- smarrimento o furto dei codici di sicurezza;
- sospetta falsificazione o abusi;
- riscontro da parte del Certificatore o dell'Ente di una violazione, commessa dal titolare, delle regole di utilizzo.

La sospensione di un certificato di firma digitale determina l'interruzione temporanea della sua validità. La sospensione ha luogo su iniziativa del Certificatore, del titolare o del Direttore Generale che ne ha autorizzato il rilascio.
La sospensione ha luogo, a titolo esemplificativo e non esaustivo, nelle seguenti circostanze:

- la possibile perdita dei codici di sicurezza;
- venir meno di uno o più requisiti che ne motivano l'assegnazione.

TITOLO VI: AMMINISTRATORI DI SISTEMA

Art.29 Definizione e requisiti di nomina

L'amministratore di sistema, ovvero il soggetto cui sono affidati i privilegi di amministratore del sistema informatico (persona fisica), è la figura professionale che provvede alla gestione, alla configurazione ed alla manutenzione della rete informatica, implementa i sistemi di sicurezza del networking nonché definisce le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte gli utenti, curando interventi di conservazione dei dati attraverso debite soluzioni di "backup" e progettando le attività di supporto al "disaster recovery".
Nell'ambito dell'organizzazione è possibile individuare tipologie specifiche di amministratore di sistema, differenziate per livello di autorizzazione e profilo.
Si possono individuare amministratori di sistema interni o esterni all'organizzazione.
L'attribuzione delle funzioni di gestore dei privilegi di amministratore del sistema informatico avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto della normativa in vigore sul trattamento dei dati e sulla sicurezza informatica.
La designazione deve essere comunque individuale e recare l'elencazione analitica degli ambiti di operatività sulla base del profilo di autorizzazione assegnato.
La designazione deve essere notificata ai soggetti individuati e dovrà in particolare individuare:

- dati identificativi del designato (nome, cognome, data e luogo di nascita, codice fiscale, residenza);
- ruolo e inquadramento nell'Amministrazione;
- profilo di autorizzazione assegnato;
- finalità dell'autorizzazione, con la specifica delle attività e dei compiti;
- l'ambito analitico di autorizzazione (fino a includere/escludere eventuali macchine, o insiemi di macchine, dispositivi, servizi, applicativi);
- riferimenti di posta elettronica e telefonici di reperibilità

Gli estremi identificativi delle persone fisiche designate quali affidatari dei privilegi di amministratore del sistema informatico, sia interni che esterni, con l'indicazione dei compiti e delle funzioni ad essi attribuite, della data di nomina e di revoca devono essere riportati in un registro conservato ed aggiornato dal Responsabile dell'USCTD.

Art. 30 Compiti funzioni e responsabilità dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico

I compiti e le funzioni dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico nell'ambito del profilo di autorizzazione assegnato, descritto nell'allegato A sono, a titolo esemplificativo e non esaustivo:

- monitorare l'infrastruttura informatica di competenza, anche attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
- proporre l'introduzione ed integrazione di nuove tecnologie negli ambienti esistenti;
- installare e configurare nuovo hardware/software sia lato client che lato server;

- applicare le patch e gli aggiornamenti necessari al software di base applicativo,
- modificare la configurazione in base all'esigenze della Amministrazione;
- gestire e mantenere aggiornati gli account utente relativi ai profili di autorizzazione;
- pianificare, eseguire e verificare la corretta esecuzione del backup e delle copie;
- documentare le operazioni effettuate, le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni a problemi, guasti e malfunzionamenti;
- operare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup secondo i criteri stabiliti dal Titolare/Responsabile del Trattamento dei dati;
- · assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;
- gestire le password di root o di amministrazione di sistema;
- collaborare con il responsabile del trattamento dei dati personali;
- collaborare con il custode delle password;
- informare titolare e responsabili sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti

Art. 31 Registrazione degli accessi e degli eventi

Gli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico saranno registrati in appositi file di log degli accessi e di altre tipologie di eventi di sistema.

Le registrazioni (access log e system log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni contengono riferimenti temporali e possono essere conservate per un congruo periodo, non inferiore a sei mesi.

Il Responsabile della sicurezza informatica provvede a controllare periodicamente, con cadenza almeno mensile, il file di log al fine di verificare il buon funzionamento dei sistemi e l'operato dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico.

È prevista la registrazione degli accessi logici da parte dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico ai sistemi client e alle workstation.

Art. 32 Divieti e disposizioni

La documentazione interna del sistema informatico dell'Ente, in particolare quella relativa all'infrastruttura di rete, alla configurazione dei sistemi e degli applicativi, alle impostazioni o abilitazioni degli utenti è conservata in luogo sicuro, preferibilmente non accessibile in rete.
L'accesso alla documentazione di cui al punto precedente è consentito esclusivamente ai soggetti cui sono affidati i privilegi di amministratore per la consultazione e aggiornamento.
È fatto divieto di trasportare la predetta documentazione fuori dalla sede dell'Ente in qualsiasi formato o supporto. Il divieto include l'invio di mail/fax/lettere contenenti documentazione anche parziale.
Gli account e le relative credenziali di livello amministratore di sistema sono segreti e non devono essere rivelati ad alcuno per nessun motivo. È fatto divieto di trasmettere in qualsiasi formato anche criptato dette informazioni.
In caso di perdita di segretezza di una credenziale di livello amministratore di sistema il soggetto cui sono affidati i privilegi di amministratore deve comunicare tempestivamente l'evento al Responsabile della sicurezza informatica; è altresì necessario annotare l'evento nel registro degli incidenti alla sicurezza,
L'amministratore di sistema dovrà agire in modo da mantenere il segreto e la riservatezza sui dati personali dei quali è venuto a conoscenza nello svolgimento delle operazioni cui è autorizzato.
Non dovrà comunicare o diffondere informazioni eventualmente acquisite durante la permanenza nei locali dell'Ente e non utilizzare documenti, dati ed informazioni acquisite durante le attività svolte nell'espletamento delle operazioni cui è incaricato per finalità che non siano ricomprese fra quelle per le quali è autorizzato;
Non dovrà comunicare o diffondere, senza la preventiva autorizzazione del Responsabile della sicurezza informatica, le informazioni relative alla situazione di sicurezza della dell'organizzazione (sistemi operativi, applicativi software, documentazione su architettura e connessioni di rete; misure e organizzazione della sicurezza).

Art. 33 Verifica attività e relazione annuale

Il Responsabile della sicurezza informatica verifica con cadenza almeno annuale l'operato dei soggetti cui sono affidati i privilegi di amministratore del sistema informatico al fine di accertarne la conformità ai compiti attribuiti e controllare la rispondenza alle misure organizzative tecniche e di sicurezza previste dalle norme vigenti. Il risultato dell'operazione di verifica, sintetizzato in una relazione, viene inviato al Responsabile dell'USCTD.

TITOLO VII: MONITORAGGIO E CONTROLLI

Art. 34 Principi generali

L'Ufficio Speciale per la crescita e la transizione digitale adotterà ogni accorgimento tecnico necessario a tutelare l'Ente da eventuali comportamenti non consentiti, salvaguardando il

rispetto della libertà e della dignità dei lavoratori. Gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

Art. 35 Monitoraggi

Il Responsabile della sicurezza informatica effettua un monitoraggio periodico del Sistema Informatico dell'Ente, al fine di:

- garantire la continuità dei servizi forniti tramite il Sistema Informatico dell'Ente
- gestire le richieste di assistenza e segnalazioni di malfunzionamento dei PC e della Rete effettuate tramite l'help desk
- garantire la protezione e ottimizzazione delle risorse di rete e il mantenimento di livelli ottimali di qualità dei servizi forniti
- garantire la protezione del patrimonio informativo, nonché l'integrità e disponibilità delle postazioni di lavoro e dei server dell'Amministrazione, rispetto a eventuali violazioni, accidentali o dolose, nel loro utilizzo;
- verificare la corretta applicazione del presente Disciplinare, per quanto di propria competenza.

Il monitoraggio di cui al presente articolo, può prevedere, limitatamente alle finalità indicate nelle specifiche Informative sulla protezione dei dati personali predisposte dall'Ente ai sensi degli artt.13 e 14 del GDPR:

- Il monitoraggio delle applicazioni software e dei sistemi;
- l'analisi del traffico di rete LAN e del traffico Internet;
- l'Inventario Hardware e Software effettuato attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete LAN dell'Ente.

Art. 36 Verifiche

In caso di anomalie, il personale incaricato dall'Ufficio Speciale per la crescita e la transizione digitale effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti regionali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.
Il personale individuato dall'Ufficio Speciale per la crescita e la transizione digitale può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete, notiziando tempestivamente le persone assegnatarie coinvolte e, comunque, nel rispetto di quanto previsto dallo Statuto dei lavoratori e dalla normativa vigente in materia di dati personali.

TITOLO VIII: RESPONSABILITÀ E SANZIONI

Art. 37 Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite

Le violazioni delle disposizioni contenute nel presente Regolamento sono fonte di responsabilità disciplinare e sono valutate, in relazione alla loro gravità, dal Responsabile dell'Ufficio o dalla struttura dell'Ente competente in materia di provvedimento disciplinare, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni a potenziale rilevanza penale ed erariale, nonché ogni eventuale uso illecito dei servizi informatici e telematici configurabili come "crimini informatici" perseguibili penalmente.

TITOLO IX: DISPOSIZIONI FINALI

Art. 38 Aggiornamento e revisione

Il presente Disciplinare è soggetto a revisione con frequenza triennale salvo innovazioni organizzative, tecniche o normative.