REGOLAMENTO INFORMATICO AZIENDALE

SOMMARIO

Premessa

Nella Napoli Servizi S.p.A. le *Tecnologie dell'informazione e della Comunicazione*[1] rappresentano da tempo strumenti di lavoro fondamentali nella propria organizzazione per il raggiungimento delle proprie finalità istituzionali.

L'utilizzo di dette tecnologie prevede l'obbligo, in osservanza dei diversi dettami legislativi, normativi e di linee guida, di stabilire alcune regole fondamentali sul corretto utilizzo della rete informatica aziendale e di tutte le risorse informatiche, al fine di prevenire l'insorgere di inconvenienti che, anche in buona fede, a vari livelli possono pregiudicarne il regolare funzionamento o addirittura arrecare danni concreti all'Azienda sotto il profilo legale, economico, operativo e di immagine.

Il presente documento costituisce così il **"Regolamento Informatico Aziendale" (RIA)**, che la Napoli Servizi adotta con l'obiettivo di aumentare la diffusione tra i propri dipendenti della cultura della sicurezza nell'utilizzo degli strumenti informatici e telematici, ispirandosi a principi di correttezza e diligenza. Esso, inoltre, si aggiunge ed integra:

- gli altri adempimenti tipici della disciplina della tutela della riservatezza in ottemperanza al d.lgs.vo 196/2003 e dal 25/05/2018 anche quanto previsto dal GDPR - Regolamento europeo in materia di protezione dei dati personali (UE) 2016/679;
- le regole di comportamento indicate nel "Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001" (MOGC) e in special modo la Parte Speciale VI.

Nel redigere questo Regolamento Informatico si è tenuto conto delle regole, degli standard e delle guide tecniche del settore e in particolare dell'Agenzia per l'Italia Digitale (AGID) per quanto previsto dalle "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

Il presente documento viene adottato, inoltre, tenendo conto di quanto previsto dalle "Linee guida del Garante per posta elettronica e internet" – emanate dall'Autorità Garante per la protezione dei dati personali, con Delibera n. 13 del 1° marzo 2007 ed in attuazione alle previsioni dell'art. 4 della Legge n. 300/1970 ("Statuto dei Lavoratori"), così come riformulato dall'art. 23 del Decreto Legislativo 14 settembre 2015, n. 151 - per fornire ai lavoratori adeguata informazione circa le modalità d'uso degli strumenti utilizzati per rendere la prestazione lavorativa e circa le modalità di effettuazione dei controlli da parte del datore di lavoro.

Il Regolamento risponde, infine, all'obbligo di adeguata informazione dei dipendenti previsto dal Decreto Legislativo n.104 del 27 giugno 2022, detto anche "Decreto trasparenza", che si propone di "disciplinare il diritto all'informazione sugli elementi essenziali del rapporto di lavoro e sulle condizioni di lavoro e la relativa tutela" e prevede specifici obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati, incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori.

[1] ICT *Information and Communication Technology*

Le indicazioni di seguito riportate hanno un diretto effetto prescrittivo e il carattere di obbligatorietà, con decorrenza dalla data di distribuzione del documento stesso.
La Napoli Servizi porrà in essere azioni di verifica al fine di monitorare l'integrità del proprio sistema informativo e il rispetto delle regole. Poiché la loro violazione, parziale o totale, dovrà ritenersi oggetto di valutazione con conseguenze proporzionate alla gravità degli atti o comportamenti assunti, è richiesta un'attenta lettura.

1. Entrata in vigore, diffusione e revisione del RIA

Il presente Regolamento entra in vigore alla data della sua approvazione, che avviene mediante Determina dell'Amministratore Unico e diffuso a tutto il personale mediante:

- affissione nella bacheca aziendale
- pubblicazione su file system aziendale accessibile a tutti gli Utenti all'indirizzo "……\dati\Transito\REGOLAMENTO INFORMATICO AZIENDALE - PROCEDURA RICHIESTE ICT"
- consegna a ciascun Utente del sistema informativo aziendale contestualmente all'affidamento della postazione informatica e/o all'erogazione delle credenziali di accesso.

Il Regolamento è soggetto a revisioni periodiche sulla base dell'evoluzione normativa e tecnologica nonché sulla base delle nuove esigenze di sicurezza e relative azioni correttive che si dovranno eventualmente intraprendere.
Le eventuali revisioni verranno approvate mediante Determinazione dell'Amministratore Unico e di tali revisioni sarà data tempestiva comunicazione agli Utenti.

Tutti gli Utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte devono essere indirizzate ai Servizi Informativi.

Tutte le disposizioni e precedenti Regolamenti in passato adottati in materia, devono intendersi abrogati e sostituiti dall'ultima versione del presente documento.

2. Campo di applicazione del regolamento

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i soggetti terzi all'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori, fornitori, stagisti, etc); costoro all'interno di questo Regolamento sono definiti Utenti.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "Utente" deve intendersi ogni soggetto in possesso di specifiche credenziali di autenticazione e più genericamente ogni utilizzatore delle tecnologie e risorse informatiche e telematiche rese disponibili dall'Azienda.

I Responsabili aziendali di ogni livello, ciascuno nell'ambito delle proprie competenze, provvedano a rendere esecutive le norme del presente Regolamento e vigilino sulla costante applicazione ed il rispetto delle disposizioni impartite, riferendo al Responsabile dei Servizi Informativi ogni eventuale esigenza emerga nella fase operativa.

Tutti gli Utenti possono rivolgersi ai Servizi Informativi aziendali oppure al proprio superiore gerarchico per ogni chiarimento, per necessità di ulteriori disposizioni particolari ovvero per la segnalazione di episodi rilevanti che si dovessero verificare durante l'utilizzo del sistema informativo.

3. Interventi tecnici di manutenzione, sicurezza e salvaguardia del sistema informatico

Il personale incaricato che opera presso il settore "Servizi Informativi" della Napoli Servizi è autorizzato a compiere interventi, nel sistema informativo aziendale, con le seguenti finalità:

- garantire la sicurezza e la salvaguardia del sistema
- monitorare l'osservanza del presente Regolamento, ovvero in caso di riscontro di abusi, come descritto in dettaglio nel paragrafo "Controlli ammessi";
- effettuare interventi tecnici e/o manutentivi (ad es. aggiornamenti del software di base, installazioni e modifiche a programmi applicativi, manutenzione hardware, configurazioni di periferiche, etc).

Detti interventi, in considerazione dei divieti enunciati nel presente documento, potranno anche comportare l'accesso, in qualunque momento, ai dati trattati da ciascuno ivi compresi gli archivi di posta elettronica, nonché la verifica dei siti Internet acceduti dagli Utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente, nelle modalità previste dalle leggi e regolamenti in materia di privacy.
L'accesso del personale dei Servizi Informativi alle postazioni di lavoro assegnate agli Utenti è limitato al tempo necessario all'espletamento dell'intervento previsto e opportunamente comunicato all'Utente stesso (in via preventiva, se possibile, oppure a conclusione dello stesso in caso di particolare urgenza).

Il personale incaricato dei Servizi Informativi ha anche 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. Tali interventi vengono effettuati esclusivamente su richiesta dell'Utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informativo. In quest'ultimo caso, e sempre che non si pregiudichi la tempestività ed efficacia dell'intervento, verrà data comunicazione all'Utente della necessità dell'intervento stesso.

Al fine di garantire l'integrità del sistema, i Servizi Informativi hanno implementato nell'infrastruttura informatica una serie di strumenti ed impostazioni che in modo anche proattivo tendono ad impedire o attenuare significativamente il rischio di abusi e minacce informatiche.

I principali strumenti e le configurazioni implementate fanno riferimento a:

- Adozione di software antivirus (in versione enterprise) su tutti i pc e server, con gestione centralizzata di aggiornamenti, avvisi e monitoraggio
- Adozione di software antivirus/antispam sui servizi di posta elettronica
- Protezione della connessione Internet con firewall ad elevato standard di sicurezza

- Sistemi per il monitoraggio del funzionamento e configurazioni dei pc e altri dispositivi di rete
- Sistemi di monitoraggio e ispezione del traffico di rete per il rilevamento avanzato delle minacce e analisi in tempo reale
- Implementazione del servizio di Web Content Filtering che consente agli Utenti la navigazione Internet solo su categorie di siti preventivamente abilitate mediante specifiche policy
- Impostazioni dell'ambiente server Microsoft Windows (Active Directory) per la gestione centralizzata dei criteri di utilizzo delle risorse informatiche condivise da parte degli Utenti
- Impostazioni dei sistemi operativi client (pc) che, attribuendo agli Utenti il ruolo di semplice user, impediscono l'alterazione delle configurazioni di sistema e delle dotazioni software installate
- Utilizzo di credenziali personali per l'accesso ai software aziendali, ricorrendo all'integrazione con il sistema di autenticazione di base di Windows (single sign-on) oppure con credenziali gestite direttamente dagli applicativi
- Sistema di videosorveglianza delle sedi.

Si evidenzia in particolare che, con il nulla osta del management aziendale e del responsabile della privacy, sono adottate specifiche tecnologie nell'ottica della prevenzione e contrasto agli attacchi e minacce mirate alla rete informatica aziendale e, più in generale, di tutela del patrimonio informativo.
Tali strumenti rappresentano una protezione dalle minacce consentendo di rilevare e analizzare gli attacchi mirati furtivi in tempo reale ispezionando il traffico di rete. Gli alert che potranno essere innescati da queste tecnologie implicano che il personale dei Servizi Informativi intervenga per verificare i dettagli delle minacce, l'origine e la destinazione e di conseguenza effettuare un controllo più puntuale sulle postazioni di lavoro, sempre esclusivamente per fini di sicurezza informatica.
Si osserva, inoltre, che l'importanza di disporre di strumenti di questo genere è dettato dalle recenti linee guida del settore e sono previste come strumenti necessari nel GDPR.

4. Finalità degli strumenti di lavoro informatici e telematici

Gli strumenti di lavoro informatici e telematici rappresentano beni aziendali affidati al singolo Utente o resi disponibili a più Utenti con finalità di strumenti di lavoro, non è quindi permesso utilizzare tali strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino leggi e normative vigenti in materia.

L'utente pertanto è tenuto, in via generale, a rispettare le seguenti prescrizioni:

1. custodire ed utilizzare le risorse informatiche e telematiche in modo appropriato, assicurandone per quanto possibile un regolare e duraturo funzionamento;
2. adoperarle esclusivamente a scopo professionale, nell'ordinario svolgimento delle proprie attività aziendali;
3. non accedere alla rete Internet per acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
4. non diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva;
5. non diffondere prodotti informativi di natura politica;

6. non diffondere in rete, o con qualsiasi altro mezzo di comunicazione aziendale, informazioni riservate di qualunque natura;
7. non svolgere qualunque tipo di attività commerciale non afferente alle finalità aziendali;
8. non compiere attività che possano rappresentare una violazione della legge in materia di diritti e copyright, fra le quali la copia non autorizzata di software, supporti audio, video etc;
9. non compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e telematiche sia aziendali sia esterna ad essa.

L'Utente deve essere consapevole che ogni utilizzo non inerente all'attività lavorativa può contribuire, anche in modo involontario, ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza del sistema informativo aziendale e anche dei sistemi informatici esterni.

5. Modalità di richiesta e assegnazione delle risorse informatiche

Per ricevere dai Servizi Informativi risorse informatiche in dotazione, per richiedere l'accesso alla rete e/o per abilitazioni all'utilizzo di servizi applicativi, è necessario attenersi alla procedura aziendale denominata "*Assistenza e supporto informatico*".

I materiali hardware e software forniti verranno consegnati agli Utenti destinatari, contestualmente alla firma per ricevuta predisposta su apposito modello che elencherà i beni assegnati.

6. Postazioni di lavoro e dotazioni

6.1 Computer

I computer sono normalmente affidati ad uso di un singolo Utente ma possono essere anche condivisi tenendo conto delle funzioni che devono essere espletate o di determinate necessità, fermo restando l'obbligo per ogni Utente di utilizzare le proprie credenziali di accesso.
I computer sono forniti con configurazioni software predefinite che non devono essere per alcun motivo modificate da parte dell'Utente.
Le richieste di installazione di nuovo software o di modifica delle configurazioni devono essere richieste dal Responsabile dell'Ufficio di appartenenza ai Servizi Informativi, che provvederà ad effettuarle previa verifica basata su elementi di disponibilità di quanto richiesto, fattibilità tecnica e accertamento di opportunità/necessità operativa.

Gli Utenti sono tenuti a:

1. non collegare dispositivi (pendrive e dischi esterni usb, smartphone, cd-rom, dvd, etc) non distribuiti direttamente dall'azienda oppure, se anche di fornitura aziendale, utilizzati precedentemente in modo promiscuo su pc non aziendali. In quest'ultimo caso, prima del loro riutilizzo, devono essere obbligatoriamente sottoposti a controllo antivirus da parte dei Servizi Informativi in ambiente isolato dalla rete (il dispositivo da controllare deve essere recapitato nell'ufficio dei Servizi Informativi);
2. non modificare la configurazione hardware della postazione di lavoro senza l'autorizzazione e il supporto degli addetti dei Servizi Informativi;

3. bloccare o disconnettere la sessione di lavoro attiva sulla propria postazione in caso di allontanamento anche per brevi periodi e assicurarsi che la schermata di blocco sia abilitata richiedendo la password per il ripristino delle attività;
4. spegnere il computer e le periferiche collegate alla fine del proprio turno di lavoro o prima di lasciare gli uffici o in caso di non utilizzo;
5. eseguire con tempestività gli aggiornamenti proposti dal sistema richiedendo l'assistenza dei Servizi Informativi se necessario;
6. non alterare le funzionalità che prevedano l'automatico aggiornamento dei componenti software presenti sulla propria postazione (es.: Windows Update), al fine di non comprometterne il regolare funzionamento;
7. non attivare funzionalità di amministrazione remota della postazione, se non esplicitamente richiesto dai Servizi Informativi;
8. non copiare sul pc file o cartelle con contenuti non attinenti alla propria prestazione lavorativa;
9. effettuare su supporti rimovibili copie di file, documenti e applicazioni solo se necessario, prediligendo piuttosto la rete aziendale (email, cartelle condivise o di transito su server) per il trasferimento verso altri uffici e per la conservazione di copie di sicurezza (backup nelle cartelle personali o di reparto sui server);
10. non asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un computer e l'altro, qualsiasi apparecchiatura in dotazione;
11. non collegare nella rete aziendale dispositivi personali o comunque dispositivi non forniti in dotazione dai Servizi Informativi;
12. dare tempestiva segnalazione ai Servizi Informativi in caso di funzionamento anomalo della postazione;
13. dare tempestiva segnalazione al proprio Responsabile in caso di danneggiamento, furto o smarrimento di dispositivi affidati, affinché ciò venga comunicato ai Servizi Informativi per le azioni conseguenti.

Nel caso di assegnazione ed utilizzo di computer portatili si applicano le stesse regole suddette con l'aggiunta che tali beni sono da custodire con particolare diligenza sia durante gli spostamenti che nell'utilizzo fuori dalle sedi aziendali.

I computer vengono forniti agli Utenti senza che essi abbiano privilegi di "amministratore locale", ad eccezione di specifiche e motivate esigenze avanzate formalmente da parte del Responsabile dell'Ufficio, sottoposte al vaglio del Responsabile dei Servizi Informativi. Tale eventuale concessione implicherà che gli Utenti dovranno prestare una maggiore e particolare attenzione nell'utilizzo della postazione per mantenere inalterati i livelli di sicurezza informatica dei sistemi interessati e della rete aziendale.

6.2 Software e configurazioni

La dotazione software della postazione informatica comprende programmi e applicativi provvisti di regolare licenza d'uso custodita a cura dei Servizi Informativi. Pertanto ogni software estraneo a quelli forniti in dotazione è da considerarsi privo di tale requisito e assimilabile a software "*pirata*" con conseguenze legali direttamente riconducibili all'utente che lo ha installato.
È opportuno precisare che anche licenze di tipo Freeware o Shareware, se valide per un uso non commerciale del prodotto, non sono idonee ad una installazione in ambito aziendale.

Gli Utenti sono tenuti a:

1. non installare programmi e applicazioni anche gratuiti che non siano tra quelli forniti a corredo della postazione di lavoro;
2. non modificare la configurazione dei software della postazione senza l'autorizzazione e il supporto degli addetti dei Servizi Informativi;
3. non disattivare, neanche temporaneamente, il firewall del sistema operativo né modificarne le impostazioni di protezione.

6.3 Protezione antivirus

Il sistema informatico aziendale è protetto da software antivirus e antispam centralizzati aggiornati continuamente. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacchi informatici mediante virus o mediante ogni altro software pericoloso.
Nel caso i software antivirus/antispam rilevino la presenza di virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale dei Servizi Informativi.
Gli utenti sono tenuti a verificare ogni giorno che il software antivirus/antispam, installato sulla postazione, sia funzionante e aggiornato, evitando categoricamente la disattivazione anche temporanea o la modifica delle impostazioni di scansione.

7. Credenziali di accesso

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale dei Servizi Informativi, previa formale richiesta del responsabile dell'Ufficio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

Ad ogni Utente viene assegnato un set di credenziali costituito da *nomeutente* e *password*, da utilizzare nelle fasi di autenticazione per l'accesso al sistema informativo aziendale, ai servizi e agli applicativi centralizzati. Per alcuni specifici applicativi potrà essere necessario fornire all'utente ulteriori set di credenziali.

Per determinati contesti tecnologici o funzionalità particolari, al processo di identificazione dell'utente basato su set di credenziali, si aggiunge obbligatoriamente l'utilizzo di un secondo fattore di autenticazione (2FA).

I Responsabili aziendali hanno l'obbligo di comunicare tempestivamente ai Servizi Informativi le variazioni in organico che comportino la revoca/modifica delle credenziali, di altre abilitazioni o privilegi di utilizzo dei sistemi informatici, al fine di inibire il processo di autenticazione o di accesso a risorse, programmi etc, per Utenti che hanno perso la titolarità ad accedere al sistema informativo o a parte di esso (es. in caso di cessazione del rapporto di lavoro, trasferimento ad altre funzioni).

Al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi, i Servizi Informativi con cadenza periodica eseguono una revisione degli Utenti e di ogni permesso e privilegio di uso delle tecnologie sottoponendo estratti di tali informazioni presenti nei diversi sistemi ai vari Responsabili dei singoli Uffici che dovranno puntualmente confermarle o fornire indicazioni in modifica.

7.1 Gestione delle credenziali di accesso

L'Utente è tenuto a conservare con la massima diligenza e segretezza i propri dati di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
Per nessun motivo deve essere consentito ad altri l'utilizzo delle proprie credenziali. Qualsiasi accesso alla rete ed ai sistemi, anche occasionale, deve prevedere l'utilizzo di credenziali personali rilasciate dai Servizi Informativi.
L'utente durante la digitazione della propria password, deve assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla e nel caso sospetti che sia stato perso il carattere di segretezza delle proprie credenziali, deve avviare tempestivamente le procedure automatiche disponibili per la modifica delle stesse e comunicarlo ai Servizi Informativi.

In ogni caso, resta inteso che l'Utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento delle proprie credenziali di accesso.

Analoga segnalazione ai Servizi Informativi va fatta dall'Utente qualora venga a conoscenza delle credenziali di un altro Utente, al fine di preservare la sicurezza del sistema informativo.

Qualora i Servizi Informativi, attraverso le normali attività di monitoraggio delle connessioni di rete rilevino l'utilizzo di credenziali da parte di soggetti diversi dall'assegnatario delle stesse, provvederanno a darne immediata comunicazione per iscritto alla Direzione aziendale e a bloccare l'utenza.

7.2 Password

La password utilizzata per l'accesso al sistema informativo deve avere le seguenti caratteristiche di complessità:

- Numero minimo di caratteri, utilizzando numeri e lettere, e con almeno un carattere speciale (ad es.: - | ? \ / #);
- Non deve contenere dati facilmente riconducibili all'utente come il nome, cognome o data di nascita;
- Non può essere uguale a password già utilizzate in precedenza per lo stesso utente;
- Deve essere modificata obbligatoriamente alla scadenza preimpostata dal sistema e dallo stesso preventivamente segnalata;
- Per ridurre al minimo i tentativi di utilizzo abusivo delle credenziali personali da parte di altri soggetti, il sistema prevede il blocco permanente dell'account dopo 5 tentativi falliti di accesso in 30 minuti (è necessario l'intervento dei Servizi Informativi per lo sblocco).

Le credenziali utente non utilizzate nell'arco di 90 giorni vengono disattivate automaticamente dal sistema e possono essere riabilitate su richiesta del responsabile dell'Ufficio di appartenenza.

Al momento dell'assegnazione delle credenziali ad un nuovo Utente, i Servizi Informativi stabiliranno una password provvisoria da utilizzare per il primo accesso con l'obbligo di contestuale modifica secondo i criteri sopra esposti.
Nel caso l'utente non ricordi più la propria password, può rivolgersi in qualsiasi momento ai Servizi Informativi per il rilascio di una nuova password provvisoria da cambiare al primo accesso.

Nei casi di necessità (esigenze di servizio, casi di prolungata assenza dal servizio, cessazione del rapporto di lavoro, etc) può essere richiesto dalla Direzione Aziendale ai Servizi Informativi di resettare la password dell'Utente per consentire l'accesso al relativo desktop del computer e alle cartelle personali sul server. Pertanto l'utente è consapevole della possibilità di accesso ai contenuti presenti su tali unità. Tale eventualità verrà preventivamente resa nota all'Utente o, nei casi di impossibilità a contattarlo, non appena possibile.

8. Utilizzo della rete aziendale e dei servizi

Le postazioni informatiche utilizzate dagli Utenti possono essere connesse stabilmente o solo occasionalmente alla rete aziendale (ad es.: collegamenti da sedi remote in VPN), per usufruire dei servizi erogati dal sistema informativo e utilizzare gli applicativi centralizzati.
Non è consentito in alcun modo il collegamento alla rete di postazioni o dispositivi diversi da quelli forniti in dotazione dall'azienda.

8.1 Profili utente

Il processo di autenticazione per l'accesso alla rete avviene da ciascuna postazione mediante l'inserimento delle proprie credenziali, a cui corrisponde un profilo utente univoco che fornisce le autorizzazioni necessarie e il grado di operatività sugli applicativi e sulle risorse condivise, basate su formali richieste dei rispettivi Responsabili di riferimento o dei vertici aziendali.

8.2 Cartelle di lavoro

Sui server centralizzati vengono messe a disposizione, per ogni settore aziendale, delle cartelle ad uso esclusivo o condiviso per l'accesso e la memorizzazione di quei dati che contribuiscono a definire il patrimonio informativo digitale, oggetto di backup periodici al fine di preservarne la disponibilità e l'integrità. La struttura di tali cartelle è predisposta dai Servizi Informativi secondo lo schema organizzativo aziendale o in base a specifiche richieste dei Responsabili degli Uffici, e a cui corrispondono autorizzazioni specifiche riconducibili al profilo utente sopra descritto.

Le cartelle di lavoro denominate "condivisa" sono accessibili dai componenti dello specifico ufficio aziendale e da soggetti che, pur non appartenendovi, hanno ricevuto la necessaria autorizzazione dal corrispondente Responsabile di riferimento.
Le cartelle personali sono invece di tipo individuale, ovvero accessibili solo dall'intestatario.

L'Utente, a riguardo, dovrà adottare le seguenti prescrizioni operative:

1. trasferire nelle cartelle sui server i dati e documenti di propria competenza che fanno parte del patrimonio informativo digitale dell'Azienda o per la cui rilevanza è necessaria la conservazione su sistemi ad alta affidabilità. Il contenuto delle cartelle, infatti, rappresenterà sempre la versione ufficiale più aggiornata dei predetti dati e documenti sia per l'accesso condiviso con altri Utenti, sia in caso di recupero per guasto o indisponibilità della postazione informatica;
2. mantenere coerente il contenuto delle proprie cartelle sui server al fine di evitare ridondanza di dati, così come l'ambiguità nelle versioni dei documenti e files non più necessari;
3. archiviare i dati e documenti di interesse comune nella cartella denominata "condivisa", in modo da renderli accessibili a tutti i componenti del gruppo di lavoro;

4. non utilizzare le cartelle di lavoro per l'archiviazione, anche temporanea, di files e cartelle non attinenti la propria attività lavorativa;
5. non trasferire sui server dati e documenti che non hanno rilevanza per l'azienda o di utilizzo transitorio;
6. eliminare tempestivamente dalla cartella denominata "Transito", utile per lo scambio occasionale di file e cartelle tra varie Uffici, i contenuti in essa creati non appena cessato lo scopo contingente. I Servizi Informativi effettueranno verifiche periodiche dei contenuti comunicandone gli esiti di volta in volta agli Utenti chiedendone l'immediata rimozione;
7. non pubblicare nella cartella "Transito" documenti contenenti dati e informazioni personali o riservate che, come tali, non devono essere rese visibili a tutti gli utenti che accedono a tale condivisa.

I Servizi Informativi hanno facoltà di rimuovere i contenuti trasferiti sui server centralizzati in violazione al presente Regolamento e/o ritenuti pericolosi per l'integrità del sistema informativo aziendale.

I Responsabili degli Uffici, anche per questo ambito, dovranno tempestivamente segnalare ai Servizi Informativi le variazioni da apportare ai profili utente, al fine di garantire la corretta gestione degli accessi alle risorse informatiche/telematiche e la coerenza delle autorizzazioni concesse su files, cartelle e applicativi centralizzati.

È a cura dei Responsabili degli Uffici indicare ai Servizi Informativi particolari esigenze di protezione e privacy che richiedano funzionalità di crittografia dei file e cartelle in gestione.

8.3 Software Applicativi centralizzati

L'utilizzo dei software applicativi centralizzati deve avvenire tenendo conto della possibilità di fruizione per il personale specificamente abilitato. È pertanto necessario che per ciascun programma software, al termine delle attività (soprattutto per quelle effettuate in modo saltuario), gli utenti chiudano l'applicativo al fine di evitare un inutile impegno delle licenze disponibili e consentire quindi la connessione ad altri utilizzatori.

9. Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti rimovibili (CD e DVD riscrivibili, supporti USB, etc), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, 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.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale dei Servizi Informativi e seguire le istruzioni da questo impartite.
In ogni caso, i supporti contenenti dati sensibili devono essere dagli Utenti adeguatamente custoditi in armadi/cassetti chiusi.

Non è consentito l'utilizzo di supporti rimovibili personali, ricevuti da terzi o, se anche di fornitura aziendale, utilizzati in modo promiscuo su pc non aziendali.

Anche i supporti rimovibili di fornitura aziendale, prima di essere utilizzati, devono essere comunque sottoposti obbligatoriamente a controllo antivirus.

10. Connessione e navigazione Internet

Al fine di limitare il più possibile i rischi derivanti dalla navigazione Internet, è necessario adottare da parte degli Utenti le prescrizioni di seguito riportate:

1. non modificare in alcun modo le impostazioni di rete e di accesso remoto del pc. In caso di problemi di connessione richiedere sempre l'intervento dei Servizi Informativi;
2. non utilizzare altri dispositivi di connettività (es.: cellulare) per effettuare connessioni alla rete Internet a meno che non si disponga di un dispositivo fornito dall'azienda o nei casi previsti come ad esempio lo svolgimento di attività in regime di lavoro agile (smartworking);
3. accedere esclusivamente a siti Internet che abbiano connessioni sicure (https e non http) e abbiano adeguate garanzie in termini di attendibilità e contenuti sicuri;
4. non accedere a siti i cui contenuti non siano di interesse per l'attività lavorativa e le mansioni affidate;
5. non modificare le impostazioni dei browser di navigazione (Chrome, etc) anche se tali modifiche vengono suggerite dai siti per una corretta fruizione dei contenuti, senza averne preliminarmente verificato l'attendibilità. Nei casi dubbi, qualora venga richiesta la modifica di dette impostazioni (applet Java, script ActiveX, etc) richiedere il supporto del personale dei Servizi Informativi per le necessarie verifiche di sicurezza prima di procedere all'eventuale attivazione;
6. non attivare alcuna funzionalità di memorizzazione delle password e/o di compilazione automatica dei moduli;
7. non utilizzare mai la stessa password per registrarsi su siti web o servizi online e per email diverse, possibilmente attivando, se prevista, l'autenticazione a più fattori (ad es. app authenticator su smartphone);
8. non effettuare download di files, documenti o applicazioni violando diritti e copyright;
9. non effettuare download di files, documenti o applicazioni non attinenti alla propria attività aziendale;
10. qualsiasi file o software scaricato deve essere verificato con l'antivirus installato sulla postazione;
11. non utilizzare il browser o altri programmi per conversazioni in chat line, forum o collegamenti con webcam se non in circostanze strettamente riconducibili al proprio lavoro;
12. non accedere a flussi audio/video in "streaming" per lunghi periodi anche se a scopo professionale, al fine di non pregiudicare la disponibilità della connessione Internet agli altri Utenti dell'azienda;
13. non effettuare registrazioni su siti Internet utilizzando i riferimenti aziendali a meno che non rientri strettamente nelle finalità della propria attività lavorativa;
14. non utilizzare il browser o altri programmi per accedere a reti "peer-to-peer" finalizzate allo scambio di file e documenti; nel caso sia necessario uno scambio di dati con altri Utenti aziendali si devono utilizzare le funzionalità interne della rete aziendale;
15. non effettuare transazioni finanziarie personali o acquisti on-line a meno che non siano previste come attività d'ufficio.

Si evidenzia, comunque, che la Napoli Servizi adotta sistemi di Web Content Filtering, basati su profili, diretti a filtrare l'accesso bloccando determinate categorie di siti o funzionalità non pertinenti all'attività lavorativa.

11. Connessione da sedi remote non aziendali

La Napoli Servizi utilizza un sistema di accesso alla rete aziendale da sedi remote (via Internet) in modalità VPN che consente agli Utenti la fruizione delle risorse informatiche con le stesse prerogative della presenza fisica in azienda. Tale facoltà, oltre a vincolare gli Utenti agli obblighi e prescrizioni già enunciate, richiede il rispetto della disciplina in ordine alle "modalità di svolgimento della prestazione lavorativa in regime di lavoro agile (smartworking)" con particolare riferimento alla riservatezza delle informazioni e al rispetto della privacy nel trattamento dei dati personali.
Tra i soggetti che utilizzano il sistema di accesso da sedi remote figurano anche fornitori, collaboratori, personale di altri enti e parti terze alla Napoli Servizi che operano in modo occasionale e/o prolungato in base alle specifiche esigenze tecniche e al rapporto stipulato con l'azienda, come meglio specificato più avanti.

Gli accessi in VPN sono consentiti ai dipendenti autorizzati che dispongono di notebook aziendali e ai fornitori autorizzati con dispositivi dotati dei previsti certificati SSL e che superino i controlli di sicurezza ed attendibilità eseguiti dai firewall aziendali.

Per detti accessi VPN è opportuno che si osservi una particolare cautela per evitare che:

- qualcuno possa osservare l'inserimento delle credenziali all'atto della connessione;
- documentazioni o dati aziendali possano essere trafugati;
- non vengano osservati i principi privacy e di protezione dei dati personali come previsto nel Regolamento Generale sulla protezione dei dati personali (GDPR);
- il dispositivo rimanga incustodito senza aver provveduto a bloccare la sessione di lavoro o aver disconnesso l'accesso alla posta aziendale.

12. Utilizzo di dotazioni informatiche personali

E' prevista, nei casi di necessità, la possibilità di utilizzare un dispositivo personale (pc, notebook, smartphone) per accedere alla posta elettronica aziendale o alle pec aziendali attraverso i portali dei fornitori di tali servizi. E' fondamentale che il dispositivo personale abbia sempre tutti gli aggiornamenti di sicurezza installati e disponga di un antivirus. Questa indicazione è ovviamente necessaria non solo per proteggere gli account di posta aziendale, ma anche quelli personali (accessi bancari, email personali, etc). Va assolutamente evitato l'uso di dispositivi pubblici o di terzi.
E' opportuno che si osservi una particolare cautela per evitare che:

- qualcuno possa osservare l'inserimento delle credenziali all'atto della connessione;
- documentazioni aziendali possano essere trafugate;
- non vengano osservati i principi privacy e di protezione dei dati personali come previsto nel Regolamento Generale sulla protezione dei dati personali (GDPR);
- il dispositivo rimanga incustodito senza aver provveduto a bloccare la sessione di lavoro o aver disconnesso l'accesso alla posta aziendale.

13. Utilizzo della posta elettronica

La Napoli Servizi utilizza sistemi di posta elettronica in cloud amministrati dai Servizi Informativi, in grado di gestire sia la messaggistica interna sia quella verso l'esterno.
Rappresentando la posta elettronica il principale strumento di comunicazione aziendale, l'assegnazione delle caselle e-mail segue lo schema organizzativo, recependo tuttavia eventuali indicazioni fornite dai Responsabili degli Uffici in base alle specifiche esigenze di servizio.

Le caselle di posta elettronica possono essere di due tipi:

- **caselle e-mail di ufficio** (ad es.: affarilegali@napoliservizi.com) - Sono da preferire per l'inoltro e la ricezione di messaggi di interesse generale del gruppo di lavoro, per questo motivo sono normalmente accessibili dalle stesse caselle e-mail personali se opportunamente autorizzati dal Responsabile dell'Ufficio;
- **caselle e-mail personali** (ad es.: inizialenome.cognome@napoliservizi.com) - Il loro ordinario utilizzo è legato all'invio e ricezione di messaggi che non necessitano di condivisione con altri componenti del gruppo di lavoro o che abbiano un requisito di riservatezza professionale.

La consultazione e la gestione delle caselle di posta elettronica possono avvenire da qualsiasi postazione collegata alla rete Internet (sia aziendale che non), con gli strumenti MS Outlook (o similari) e web mail mediante il browser Internet in uso. I messaggi ricevuti ed inviati da qualsiasi casella e-mail, permanendo sui server - in modo da consentire le ordinarie attività di gestione dei servizi di posta elettronica - saranno sempre disponibili anche se scaricati su una specifica postazione di lavoro.

Indipendentemente dalla modalità scelta, l'utilizzo delle caselle di posta elettronica è disciplinato dalle seguenti prescrizioni:

1. la casella di posta elettronica aziendale viene concessa per un utilizzo professionale. Le responsabilità derivanti da un uso diverso sono da ascriversi esclusivamente all'utente assegnatario;
2. l'Utente è tenuto a consultare regolarmente la casella di posta elettronica di propria competenza;
3. non è consentito inviare tramite e-mail informazioni e/o allegati di particolare rilevanza strategica per l'azienda, poiché non è possibile garantire la certezza di identità del destinatario e le finalità di utilizzo di tali informazioni. In tali casi è opportuno utilizzare messaggi pec.
4. non è consentita l'iscrizione a mailing list non professionali e l'inoltro di messaggi relativi a "catene di S. Antonio" e simili;
5. è vietata l'apertura e/o la memorizzazione di file allegati ai messaggi di posta elettronica provenienti da mittenti sconosciuti o di dubbia identità, a causa dell'elevata diffusione di minacce alla sicurezza del sistema informativo costituite da virus, spyware, trojan, adware, etc;
6. per i messaggi provenienti da mittenti attendibili, l'apertura e/o memorizzazione di file allegati deve essere sempre preceduta dalla scansione con il software antivirus residente sulla postazione informatica, al fine di scongiurarne la pericolosità derivante da un'inconsapevole presenza di virus sulla postazione del mittente;
7. è vietata la reimpostazione della disattivazione in esecuzione/apertura automatica di messaggi e macro;

8. utilizzare sempre i formati compressi (es.: zip, rar) per ridurre le dimensioni dei file allegati ai messaggi di posta inviati;
9. in ogni caso, tenere conto che per il sistema di posta aziendale la dimensione massima degli allegati è pari a 35 Mb. Qualora necessario, inviare più messaggi contenenti allegati di dimensioni inferiori alla massima consentita.

Per gli aspetti formali è opportuno tenere conto anche delle seguenti indicazioni:

1. scrivere sempre l'oggetto del messaggio evitando di utilizzare oggetti di altre email non rispondenti al contenuto che si intende comunicare;
2. firmare il messaggio soprattutto nei casi di utilizzo della casella di posta di ufficio, specificando il proprio ruolo rispetto all'organizzazione ufficiale (fare riferimento al proprio ordine di servizio per l'utilizzo dei termini: responsabile, supervisore, addetto etc);
3. il modello di firma standard da utilizzare è disponibile nell'area condivisa sui server ".....\dati\Transito\MODELLI DOCUMENTI AZIENDALI" (file firma-email.dot);
4. non utilizzare template o elementi grafici personalizzati;
5. il font da preferire è Garamond – dimensione 11;
6. fare attenzione all'uso dello stile dei caratteri usando il grassetto/sottolineato per evidenziare solo i punti salienti del messaggio;
7. nelle risposte/inoltri seguire il principio della "piramide rovesciata" – il testo che si sta redigendo va collocato all'inizio del messaggio.

Allo scopo di facilitare l'interscambio di informazioni all'interno dell'Azienda è previsto l'uso delle liste di distribuzione presenti nella rubrica centralizzata. Occorre incentivare e favorire l'uso di tali liste evitando in tal modo, nell'inviare delle e-mail, eventuali omissioni o errate inclusioni di destinatari. Al fine di non duplicare le comunicazioni è opportuno anche che una comunicazione e-mail inviata ad una lista di distribuzione non venga anche contemporaneamente inviata alla e-mail individuale.

Le richieste di attivazione di una lista di distribuzione possono essere avanzate da un Responsabile di Ufficio e contenere l'elenco dei nominativi che devono essere inseriti nella relativa lista di distribuzione. Resta in capo al Responsabile richiedente la verifica, almeno annuale, della necessità di mantenere attive le liste di distribuzione a lui afferenti e l'elenco dei nominativi abilitati.

In caso di necessità (esigenze di servizio, casi di prolungata assenza dal servizio, cessazione del rapporto di lavoro, etc) può essere richiesto dalla Direzione Aziendale ai Servizi Informativi di resettare la password per consentire l'accesso alla casella e-mail. Pertanto l'utente è consapevole della possibilità di accesso ai contenuti dei messaggi inviati e ricevuti tramite la propria casella di posta elettronica. Tale eventualità verrà preventivamente resa nota all'Utente o, nei casi di impossibilità a contattarlo, non appena possibile.

In caso di cessazione del rapporto di lavoro da parte di dipendenti o di altri soggetti incaricati (in seguito ad es. a pensionamento/dimissioni, conclusione della collaborazione etc), a seguito di segnalazione del rapporto cessato da parte dell'Area Risorse Umane e Organizzazione, i Servizi Informativi provvedono a disattivare l'account di posta del lavoratore/soggetto cessato; con modalità automatizzate i terzi vengono informati che l'account dell'utente è stato disattivato.

Decorso un tempo congruo a garantire la continuità del servizio (individuato, salvo situazioni particolari, in 12 mesi come stabilito dall'Amministratore Unico nella nota protocollo tra funzioni n. 235/2024 del 30/10/2024), i Servizi Informativi procedono alla cancellazione definitiva dell'account.

La conservazione dei messaggi email inviati e ricevuti dall'account è consentita all'Azienda per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti di legge.

I metadati relativi alle operazioni di invio e ricezione e smistamento dei messaggi email sono detenuti dal fornitore della posta elettronica e da questi conservate fino a 90 giorni per assicurare il funzionamento delle infrastrutture del sistema della posta elettronica e per poter gestire e risolvere eventuali problematiche tecniche legate al suo corretto funzionamento.

14. Utilizzo della piattaforma Teams

La Napoli Servizi ha adottato il software Microsoft Teams come strumento di collaborazione tra i componenti delle funzioni aziendali e in generale per favorire la gestione e l'organizzazione delle comunicazioni in un unico punto.
Teams è infatti una piattaforma integrata in MS Office che combina chat di lavoro persistente, videoconferenze web (audio o video), condivisione schermo, ed altre funzionalità.
Tutti i dipendenti con account aziendale sono abilitati all'utilizzo di Teams nelle sue varie modalità (browser web, app Windows e mobile per iOS e Android) mediante l'utilizzo delle proprie credenziali personali di accesso alla rete aziendale con l'aggiunta del secondo fattore di autenticazione (app authenticator).

15. Utilizzo di fax, stampanti e fotocopiatrici aziendali

Al fine di perseguire l'obiettivo di progressiva dematerializzazione dei documenti ed archivi cartacei e il relativo contenimento dei costi, corre l'obbligo di limitare il più possibile le attività di stampa, prediligendo in tutti i casi possibili la consultazione, la conservazione e il trasferimento dei documenti in formato elettronico.

In ogni caso si devono preferire le stampanti di rete di tipo dipartimentale che hanno costi di esercizio inferiori rispetto ad altri dispositivi di stampa. Detti dispositivi sono stati programmati per eseguire le stampe in modalità riservata dalle postazioni di lavoro in modo che possano essere ritirate solo dall'utente che ha eseguito il lavoro.

Per tutti i materiali di consumo: toner, cartucce ink jet, carta per stampanti, se ne raccomanda un uso per finalità strettamente necessarie evitando sprechi o utilizzo eccessivo.

Va inoltre precisato che le stampanti di rete di tipo dipartimentale consentono di risalire al nominativo degli Utenti e al numero di stampe effettuato.

In particolare è richiesta l'osservanza dalle seguenti prescrizioni:

- È vietato l'utilizzo dei fax, delle fotocopiatrici e stampanti aziendali per fini personali o comunque non inerenti alla propria attività lavorativa;

- Nell'eseguire fotocopie o scansioni, accertarsi che i fogli siano privi di punti metallici, fermagli, adesivi che possano bloccare e danneggiare il dispositivo;
- Se viene utilizzato correttore liquido (bianchetto), assicurarsi della completa essiccazione sugli originali prima di effettuare fotocopie/scansioni al fine di non macchiare l'unità ottica di acquisizione;
- Per problemi di inceppamento carta è necessario procedere all'estrazione della carta in maniera delicata usando le apposite rotelle e mai muovendo i fogli contro il loro naturale movimento; nei casi di utilizzo delle stampanti/fotocopiatrici dipartimentali bisogna seguire le indicazioni che appaiono sul display del dispositivo, e nei casi particolari contattare sempre i Servizi Informativi;
- Ritirare le stampe non appena inviato il lavoro, eventualmente eliminando o interrompendo quelle eseguite per errore o non più necessarie;
- Nei limiti del possibile utilizzare la stampante in modalità fronte-retro e in modalità bianco e nero.

In termini generali gli Utenti devono attenersi ad un disciplinato uso dei dispositivi di stampa, ribadendo che si deve ricorrere alle stampe/fotocopie (e in particolare a quelle a colori) solo per i reali casi di necessità, considerando che l'Azienda dispone di diversi altri strumenti di accesso, condivisione e diffusione di documenti (e-mail, cartelle condivise, cartelle di transito).

16. Modelli e templates di documenti informatici

Una efficace gestione dei documenti elettronici aziendali è strettamente relazionata all'esistenza di modelli strutturali e contenutistici condivisi all'interno dell'organizzazione. Sono state pertanto adottate delle regole nella creazione/modifica dei documenti sia per l'editing formale sia per il versioning dei contenuti in modo che ogni utente possa ricondursi ad un medesimo standard che faciliti condivisioni, collaborazioni e corretta comprensione dei documenti comuni.

La Napoli Servizi ha per questo individuato dei requisiti di uniformità delle documentazioni aziendali introducendo delle tipologie di modelli di files che dovranno essere utilizzati rispettando le regole di seguito indicate:

- Utilizzare i modelli predisposti nell'area condivisa sui server (……\dati\Transito\MODELLI DOCUMENTI AZIENDALI), selezionando quello rispondente al documento da redigere (lettera, progetto-relazione, modulo etc), senza alterare i logo e le impostazioni standard, adattandoli alle proprie esigenze di stampa A4/A3 – orientamento orizzontale/verticale;
- Nel nome file di ogni documento (Word, Excel, Pdf etc) deve essere indicato: l'ufficio, il titolo del documento e la versione separati da un trattino (ad es. AFC-Budget2018-Ver.1.0.docx);
- Ogni documento di tipo relazione/progetto deve riportare nel piè di pagina:
  - a destra i numeri di pagina nel formato "pag. 1 di 2"
  - a sinistra: l'ufficio, il titolo del documento, la data e la versione (vedasi ad es. il piè di pagina del presente documento);
- Per le lettere prevedere solo il numero di pagina a destra, specificando, nel caso venga richiesto dal proprio Responsabile/Dirigente, l'apposizione a sinistra della propria sigla personale che possa ricondurre successivamente all'autore;

- Per ogni revisione dello stesso documento deve essere incrementata la versione (anche nel nome file) e aggiornata la data se diversa;
- Utilizzare come testo standard (ad es. per il corpo di una lettera) il font Garamond corpo 11;
- Utilizzare i font standard presenti in Word per definire i Titoli (H1, H2, etc) e Sottotitoli;
- Utilizzare l'interlinea e spaziatura standard prevista in Word;
- Utilizzare i punti elenchi e punti numerati standard presenti in Word;
- Utilizzare la funzionalità di Word per costruire Sommari e Indici;
- Formattare le tabelle con i font standard suddetti e ponendo i titoli delle colonne in maiuscolo. Utilizzare, nei limiti del possibile, sfondi in sfumature di grigio per le righe/colonne;
- Assicurarsi che il documento proponga margini coerenti e dimensioni delle tabelle uniformi, a meno che non sia necessario diversamente;
- Inoltre si tenga conto che i documenti possono essere distribuiti in formato Office (Word, Excel etc) o in formato di file salvato come Acrobat (.pdf), che diversamente dai pdf scansiti (che sono delle immagini) ne consentono ancora la gestione dei contenuti (es. ricerca e copia di testo).

In caso di particolari esigenze potranno essere temporaneamente utilizzati template alternativi, purché includenti il logo aziendale e previa approvazione della Direzione Aziendale.

Per la produzione di documentazioni nei formati aperti, si rimanda alla consultazione della guida presente nell'area condivisa summenzionata in questo capitolo.

17. Rapporti con parti terze alla Napoli Servizi (fornitori, collaboratori, personale di altri enti...)

I fornitori, collaboratori, personale di altri enti e parti terze alla Napoli Servizi che utilizzano i sistemi informatici e telematici aziendali, devono impegnarsi a rispettare gli obblighi di legge in tema di reati informatici. A tal uopo, i predetti soggetti sono, altresì, tenuti all'osservanza delle clausole inserite nei relativi contratti dagli stessi sottoscritti, così come previsto dal/i Regolamento/i aziendale/i di riferimento.

In tal ottica gli Utenti aziendali, nell'interagire con fornitori, collaboratori etc, devono segnalare ai Servizi Informativi ogni eventuale comportamento inadeguato che venga rilevato.

Per l'utilizzo del collegamento alla rete e per l'utilizzo degli applicativi aziendali della Napoli Servizi S.p.A. da parte di terzi (ad esempio dipendenti del Comune di Napoli) è necessario che venga compilato e sottoscritto da ogni utilizzatore il modulo di "Assunzione di Responsabilità", che è parte integrante del presente Regolamento. Il modulo dovrà essere consegnato al settore Servizi Informativi che preventivamente valuterà l'esistenza delle dovute autorizzazioni e la fattibilità tecnica.

18. Controlli ammessi

18.1 Tipologia e finalità

Sono ammesse le forme di controllo volte a tutelare il patrimonio informativo aziendale, la sicurezza delle risorse informatiche, la manutenzione dei sistemi informativi, di rete nel rispetto dei criteri nel prosieguo indicati.

Sono altresì ammesse, nel rispetto dei criteri nel prosieguo indicati, forme di controllo volte a verificare il rispetto delle regole di utilizzo delle risorse tecnologiche di informazione e comunicazione da parte dei dipendenti, così come chiarite nel presente Regolamento e divulgate a tutto il personale della Napoli Servizi, senza distinzione di ruolo e/o livello.
Il compimento dei suddetti controlli, pertanto, ha carattere di eccezionalità, occasionalità, temporaneità e ha fini meramente "difensivi". Il personale incaricato del Settore Servizi Informativi accede ai dati delle comunicazioni telefoniche o telematiche nel caso in cui ci sia il fondato sospetto di gravi abusi o illeciti e, in ogni caso, previa autorizzazione della Direzione Aziendale, nel rispetto e nei limiti di quanto previsto per legge.

Il personale coinvolto nelle attività di controllo è tenuto al segreto professionale per le informazioni acquisite nello svolgimento di tale attività.

18.2 Controlli in forma anonima

Nei limiti delle finalità suindicate, i controlli sono generalmente ispirati ai principi di proporzionalità, equità e trasparenza, riguardano dati generali aggregati in forma anonima e non sono riferibili ai singoli lavoratori.

18.3 Controlli individuali

Nell'ipotesi in cui l'attività di controllo determini l'accertamento di abusi o comportamenti illeciti e si riscontri la loro reiterazione, sono eseguite verifiche più approfondite, onde appurare eventuali responsabilità individuali.

L'attività di accertamento appena esposta è condotta in modo graduale, secondo un criterio che utilizza aree di riferimento progressivamente puntualizzate, ed è preceduta, nell'imminenza del suo compimento rispetto al singolo Utente o ad un gruppo ristretto di essi, dall'informazione agli interessati.

18.4 Controlli sollecitati dall'Autorità Giudiziaria

Le verifiche di cui al paragrafo precedente possono essere compiute su richiesta dell'Autorità Giudiziaria.

19. Competenze, responsabilità e sanzioni

Il **Responsabile dei Servizi Informativi** è tenuto a:

- Elaborare le regole per un utilizzo ragionevolmente sicuro del sistema informativo aziendale;
- Implementare con l'ausilio del personale dell'Ufficio o del personale reso disponibile dai fornitori incaricati, le regole di sicurezza sul sistema informativo aziendale;
- Monitorare, con l'ausilio del predetto personale, i sistemi per individuare un eventuale uso scorretto degli stessi o difforme da quanto disposto nel presente Regolamento o in ogni caso in violazione di leggi e regolamenti;
- Segnalare prontamente alla Direzione Aziendale ogni eventuale attività non autorizzata sul sistema informativo della Napoli Servizi.

I **Responsabili degli Uffici aziendali** sono tenuti a:

- Informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo aziendale;
- Assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente Regolamento;
- Assicurare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente Regolamento;
- Adempiere a tutti gli obblighi inerenti alla responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dall'Azienda;
- Segnalare prontamente al Responsabile dei Servizi Informativi ogni eventuale attività non autorizzata sui sistemi informatici e telematici citati nel presente Regolamento.

Il **Personale dei Servizi Informativi e l'eventuale personale esterno incaricato** che concorre alla gestione/implementazione del sistema informativo dell'Azienda sono tenuti a:

- Garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
- Segnalare prontamente al Responsabile dei Servizi Informativi ogni eventuale attività non autorizzata sui sistemi informatici e telematici citati nel presente Regolamento.

In modo strettamente limitato a quanto necessario per il corretto svolgimento delle proprie funzioni, il personale dei Servizi Informativi è esentato dall'applicazione del presente Regolamento.

Agli **Utenti dei sistemi informatici e telematici dell'Azienda** è fatto obbligo l'applicazione e il rispetto puntuale delle disposizioni contenute nel presente Regolamento e l'adempimento di tutti gli obblighi inerenti alla responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dall'Azienda. Il mancato rispetto e/o la violazione delle regole ivi contenute sono perseguibili disciplinarmente, ai sensi del CCNL e del Codice Disciplinare interno, oltre che in sede legale, mediante la promozione, da parte della società, di ogni adeguata azione tesa ad ottenere il risarcimento di qualsiasi danno e/o pregiudizio che dovesse derivarne per l'azienda.