Regolamento interno per l’uso dei sistemi informatici

Approvato dal Consiglio Direttivo con delibera 110/2025 del 19/06/2025

Approvato dal Comitato Centrale FNOPI in data 14/11/2025

Lista di distribuzione

Destinatari	Forma	Data
Personale amministrativo dell’OPI di Vicenza	Consegna cartacea	19/11/2025
Organi dell’Ordine	Trasmissione PEC	19/11/2025
Iscritti all’Ordine	Pubblicazione sito web	19/11/2025

Revisioni

Rev.	Data	Motivazione	Gruppo di lavoro	Approvazione
1	19/06/2025	Stesura	*Presidente* Giacomo Sebastiano Canova *Vicepresidente* Fabio Carollo *Segretario* Barbara Pozza	*Presidente* Giacomo Sebastiano Canova

Regolamento interno per l'uso dei sistemi informatici

SOMMARIO

Regolamento interno per l'uso dei sistemi informatici

Articolo 1- Premessa
Al fine di stabilire alcune regole di condotta, necessarie per operare in un conveniente regime di sicurezza, di rispetto delle norme di legge e di contratto, l'Ordine delle Professioni Infermieristiche (di seguito OPI) di Vicenza ha predisposto il seguente regolamento interno che disciplina l'utilizzo di ogni sistema informatico.
La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla Rete Internet espone l'OPI di Vicenza a rischi di natura patrimoniale e penale correlata a violazioni delle norme in materia di tutela dei dati personali.
Premesso che l'utilizzo delle risorse informatiche deve sempre ispirarsi al principio della diligenza e correttezza (comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro), l'OPI di Vicenza, con l'adozione del presente regolamento interno, intende evitare che inconsapevoli comportamenti possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Articolo 2 - Riferimenti
Il presente regolamento si ispira al quadro normativo vigente in materia di tutela dei dati personali, sicurezza informatica e diritti dei lavoratori. Di seguito sono elencati i principali riferimenti normativi e regolatori:
- Legge 300/1970 (Statuto dei Lavoratori);
- D.Lgs.231/2001;
- Reg.UE 679/2016
- Videosorveglianza-provvedimento a carattere Generale del 8 aprile 2010 [doc Web 1712680];
- Linee guida del Garante per posta elettronica e Internet 1 marzo 2007 [doc. web n. 1387522];
- Linee-guida per il trattamento di dati dei dipendenti privati - 23 novembre 2006 [doc web n. 1364099]
- Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati n. 243 del 15 maggio 2014 [doc. web n. 3134436]

Articolo 3 - Entrata in vigore
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Copia del regolamento è a disposizione di ciascun dipendente presso la sede.
Il regolamento entra in vigore il giorno successivo alla sua approvazione da parte del Comitato Centrale della Federazione Nazionale.

Articolo 4 - Scopo e campo di applicazione
L'applicazione del presente regolamento interno garantisce il miglioramento materiale e immateriale delle condizioni di sicurezza funzionali alla protezione dei dati personali e patrimoniali e si applica, in fase di utilizzo, a qualsiasi sistema informativo che operi o sia interconnesso alla Rete informatica, al personale dipendente o terzo assegnatario di attrezzatura informatica in comodato d'uso.
Le informazioni eventualmente acquisite dall'OPI di Vicenza attraverso l'uso degli strumenti di lavoro sono utilizzabili per tutte le finalità connesse al rapporto di lavoro (anche terziarizzato con obbligo di riservatezza), ivi compresa l'instaurazione di procedimenti disciplinari, ai sensi dell'art. 4, L. 300/70, così come sostituito dall'art. 23 del D.lgs. 151/2015, e rappresenta informativa utile ad avvisare gli utilizzatori circa il trattamento dei dati acquisiti dal datore di lavoro nell'ambito della

prestazione lavorativa attraverso le dotazioni di servizio e le strumentazioni associate a tali strumenti.

Articolo 5 - Destinatari

Il presente regolamento interno si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'OPI di Vicenza, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, etc.) e ai membri degli Organi dell'Ente nell'esercizio delle loro funzioni.
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione.
Tale figura corrisponde inoltre a quella dell'Autorizzato al Trattamento.
Gli assegnatari del PC Portatile devono ispirarsi ad un principio generale di diligenza e correttezza nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo.

Articolo 6 - La rete informatica

Il patrimonio informativo utilizza, per il trasporto dei dati, una piattaforma di Rete che, per il suo funzionamento, viene gestita ricorrendo a soggetto terzo specializzato ("Amministratore del Sistema" regolarmente contrattualizzato come Responsabile del Trattamento articolo 28 del GDPR).
Si elencano di seguito alcune prescrizioni operative:

- le unità di Rete sono aree/spazi di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi; pertanto qualunque file non riconducibile all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; su queste vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema;
- l'accesso alle condivisioni di rete è consentito con l'autenticazione dell'utente al dominio di rete. I diritti di accesso in lettura/scrittura nelle cartelle sono gestiti dall'Amministratore del Sistema (anche se esterno);.
- ogni utilizzatore di unità di Rete dovrà effettuare la pulizia dei propri archivi evitando la presenza di files obsoleti o inutili; particolare attenzione deve essere prestata alla duplicazione dei dati: è assolutamente da evitare un'archiviazione ridondante;
- limitare la stampa in Rete di documenti con dati personali e sensibili per evitare la diffusione di notizie, documenti ecc.., nel caso, ritirarla prontamente dai vassoi delle stampanti comuni; laddove possibile impostare le password di stampa sul dispositivo.
- per l'accesso alla Rete ciascun utente deve essere in possesso della specifica credenziale di autenticazione;
- 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;
- si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio automatico; la responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente;
- il personale addetto alla gestione della Rete può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di Rete.

Regolamento interno per l'uso dei sistemi informatici

Articolo 7 - Gestione ed assegnazione delle credenziali di autenticazione
Le credenziali di autenticazione per l'accesso alla Rete vengono assegnate con formale richiesta del Responsabile dell'Area nell'ambito del quale la risorsa andrà ad operare come "nuovo utente".
Nel caso di collaboratori esterni la preventiva richiesta verrà inoltrata direttamente dalla Direzione (ovvero dal Responsabile dell'Area con il quale il collaboratore si coordina nell'espletamento del proprio incarico).
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Autorizzato al trattamento con la massima diligenza e non divulgata. Non è consentita la modifica della password di accensione (BIOS) se non autorizzata dall'Amministratore del Sistema.
La parola chiave (formata da lettere maiuscole o minuscole e/o numeri, anche in combinazione fra loro) deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'Autorizzato al trattamento (cfr: l'utilizzatore del PC o del Device).
È necessario procedere alla modifica della parola chiave a cura dell'utente, Autorizzato al trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi.
Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale dedicato.
Il Soggetto preposto alla custodia delle credenziali di autenticazione è l'amministratore delle reti.

Articolo 8 - Esempio di scelta password utente
La password è lo strumento che consente l'accesso ai sistemi informatici in uso.
Affinché il Sistema di autenticazione al Dominio ritenga valida la password adottata, fin dal principio, dovranno essere rispettati i seguenti criteri:

a. dovrà essere composta da almeno 8 caratteri;
b. non deve contenere il nome, il cognome o lo User Name dell'utente;
c. non deve contenere riferimenti all'OPI di Vicenza.

Articolo 9 - Utilizzo delle apparecchiature informatiche (personal computer, personal computer portatile, Tablet)
L'OPI di Vicenza favorisce la piena connettività in Rete Intranet ed Internet delle risorse operanti per suo conto tuttavia, per ottimizzare l'efficienza e la sicurezza al trattamento dei dati personali e patrimoniali, ogni utilizzatore dovrà attenersi alle seguenti prescrizioni consapevole che il Titolare dell'Informazione, per garantire la piena sicurezza della Rete, si riserva di superare ogni accesso e limitazione predisposta (ad esempio password, E-Mail, dischi di Rete).
Si elencano di seguito alcune prescrizioni operative a cui ogni utilizzatore deve attenersi:

- l'apparecchiatura affidata al dipendente è uno strumento di lavoro; ogni utilizzo non inerente all'attività lavorativa può contribuire a creare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza patrimoniale;
- l'utilizzo del PC o di ogni altro mezzo di elaborazione dati per scopi personali dai quali l'utilizzatore tragga o meno un vantaggio economico personale può rappresentare un uso indebito dello strumento di lavoro per il quale possono applicarsi le previste sanzioni disciplinari (rif.: CCNL) o contrattuali nel caso di terzi;
- il bene deve essere custodito con cura evitando ogni possibile forma di danneggiamento;

Regolamento interno per l'uso dei sistemi informatici

- l'accesso all'elaboratore, alle applicazioni con dati sensibili, patrimoniali, personali, per l'uso di Internet, è subordinato all'adozione di idonea password conosciuta e custodita dall'Autorizzato al trattamento con la massima diligenza e non divulgata;
- evitare assolutamente l'installazione autonoma di programmi provenienti dall'esterno, salvo autorizzazione esplicita dell'Amministratore del Sistema;
- evitare l'uso di programmi diversi da quelli distribuiti ufficialmente;
- evitare la modifica delle caratteristiche software e hardware predisposte per il proprio PC, salvo autorizzazione esplicita dell'Amministratore del Sistema;
- chiudere correttamente ogni sessione aperta e successivamente spegnere ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio il proprio PC, bloccare il Tablet (*in caso di assegnazione come dotazione personale*) con sistemi di cifratura o segno;
- prima di lasciare incustodito l'elaboratore utilizzare l'apposita password con lo screen saver chiudendo preventivamente l'abilitazione alle applicazioni (ad esempio Crtl+Alt+Canc per Windows);
- il personale incaricato formalmente alla gestione della infrastruttura informatica, per l'espletamento delle sue funzioni, per garantire la sicurezza del sistema informatico e per garantire la regolarità del servizio del lavoro, ha la possibilità, in qualunque momento, e su imposizione del Titolare dell'Informazione, di accedere ai dati dell'OPI di Vicenza trattati da ciascuno, ivi compresi gli archivi di posta elettronica; la stessa facoltà, sempre e solo ai fini della sicurezza del sistema e per garantire la normale operatività dell'OPI di Vicenza, si applica anche in caso di assenza prolungata od impedimento dell'utente; analoghe verifiche possono essere effettuate sui siti internet visitati dagli utenti abilitati alla navigazione esterna; l'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo del lavoratore a distanza;
- non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'OPI di Vicenza, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'OPI di Vicenza a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software vengono sanzionate anche penalmente essendo a carico dell'OPI di Vicenza le sanzioni amministrative elevate in caso di accertamento d'illecito;
- il personale Autorizzato al servizio di gestione della Rete (ovvero l'Amministratore del sistema) ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni 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;
- non è consentita l'installazione autonoma sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio, masterizzatori, modem, ecc.);
- segnalare immediatamente all'Amministratore del Sistema l'eventuale presenza di virus informatici ed ogni altra anomalia riscontrata;
- è vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica su aree di Rete.

Regolamento interno per l'uso dei sistemi informatici

Articolo 10 - Utilizzo di PC portatili

L'utente è responsabile del PC portatile e di ogni altra attrezzatura ad esso assegnata, che deve custodire con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in Rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Si ricorda, in conformità alle norme di legge sulla tutela delle notizie riservate e della privacy, e tenendo in debito conto che tali strumenti informatici e dispositivi sono strumenti di lavoro, posti dall'OPI di Vicenza nella disponibilità dei lavoratori e terzi collaboratori, che tali strumenti devono essere usati esclusivamente per le finalità connesse all'esecuzione della prestazione lavorativa.

È espressamente vietato ogni utilizzo del sistema informatico per finalità diverse da quelle strettamente professionali.

L'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo del lavoratore a distanza.

L'accesso al sistema informatico assegnato - ed alle estensioni logiche dei programmi installati - è effettuato eventualmente dalla Segreteria, con il supporto della Società esterna di manutenzione del sistema informatico o dell'amministratore delle reti, nel rispetto delle misure di sicurezza previste dal Codice della privacy e di inerenza con la finalità di eventuale indagine dell'evento.

Al di fuori delle indicate finalità e, fatti salvi i casi di necessità e urgenza, l'accesso è consentito solo previo avviso all'utente o al suo fiduciario o su richiesta degli stessi.

L'accesso all'elaboratore è protetto da un sistema di autenticazione. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza.

È installato un software antivirus per prevenire eventuali attacchi informatici o prevenire azioni di ricerca "riscatto oneroso" (esempio Ramsomware, Wanna Cry) che possano provocare danneggiamenti al software, causati dalla presenza o dall'azione di programmi virali. Pertanto, qualora si evidenzino anomalie di funzionamento del computer, è obbligatorio segnalare l'evento all'Amministratore del Sistema.

Le unità di rete e le aree di condivisione (autorizzate nei casi di soggetti terzi esterni all'OPI di Vicenza) contengono informazioni strettamente professionali e non possono essere utilizzate per scopi diversi.

Il personal computer portatile deve essere spento al termine dell'attività lavorativa o in caso di assenze prolungate dall'ufficio. Non è consentita la copia o la trasmissione dei dati tramite dispositivi di memorizzazione, comunicazione o altro, se non con l'autorizzazione espressa dell'Amministratore del Sistema.

I servizi online devono essere esclusivamente finalizzati al reperimento di informazioni utili allo svolgimento del rapporto di lavoro. Ogni altra utilizzazione dell'accesso su internet, non finalizzata al reperimento di informazioni utili allo scopo indicato, e non pertinente all'attività lavorativa o di tipo personale, non è consentita.

Al fine di non compromettere la sicurezza dell'OPI di Vicenza e di prevenire conseguenze legali o di altro genere, gli utenti dovranno adottare i seguenti comportamenti:

- non scaricare software gratuiti (freeware) e shareware prelevati da siti Internet, se non espressamente autorizzati dall'Amministratore del Sistema;
- è vietata l'effettuazione di ogni genere di transazione finanziaria (personale) ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto lavorative;

- è vietata ogni forma di registrazione e partecipazione a siti o social network (personali), i cui contenuti non siano legati all'attività lavorativa;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat, di bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti allo svolgimento del rapporto di lavoro.

Si ribadisce che il Pc portatile assegnato al dipendente o eventualmente a soggetto terzo per motivi di servizio in comodato d'uso, per le funzioni e mansioni previste, è un bene di proprietà dell'OPI di Vicenza ai sensi degli artt. 1803 e seguenti del Codice Civile (vedasi: contenuti della modulistica in vigore per la gestione del comodato d'uso di bene - consegnato).
La restituzione del bene potrà essere richiesta dall'OPI di Vicenza in qualunque momento.
Il Pc portatile non potrà essere ceduto a terzi ad alcun titolo, neanche temporaneamente.
L'assegnatario è responsabile dell'utilizzo e della custodia del Pc portatile e dei relativi accessori secondo l'ordinaria diligenza (a titolo esemplificativo non lasciando incustodito il Pc Portatile all'interno dell'autovettura).

Articolo 11 - Utilizzo e conservazione dei supporti rimovibili

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.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale addetto e seguire le istruzioni da questo impartite. In ogni caso, tali supporti magnetici devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
È vietato l'utilizzo di supporti rimovibili personali sulla rete ed apparecchiature di lavoro.
L'utente è responsabile della custodia dei supporti di memorizzazione e dei dati in essi contenuti.

1. Supporti di memorizzazione (HD rimovibili, Chiavette USB, ecc.)

Nell'ambito della quotidianità d'uso delle tecnologie informatiche potrebbe essere necessario ricorrere all'utilizzo di supporti magnetici riutilizzabili (HD rimovibili ,USB etc.) in grado di contenere anche dati sensibili o riguardanti il patrimonio dell'OPI di Vicenza.
Tali supporti devono essere trattati per evitare l'eventuale recupero dei dati da parte di soggetti non autorizzati o terzi con la conseguente esposizione debitoria, d'immagine e penale
In particolare, devono essere custoditi in "contenitori" ovvero archivi chiusi a chiave (basta anche un cassetto chiuso).
Tutti i supporti USB (di memoria) prima di essere utilizzati all'interno del sistema, devono essere necessariamente validati dall'amministratore di sistema.
Non è consentito:

- l'utilizzo, non autorizzato, di supporti magnetici di provenienza ignota (chiavette USB, hard disk esterni, CD-ROM, DVD, ecc.);
- scaricare nella Rete dell'OPI di Vicenza files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Non viene raccomandata la copia su memorie USB di dati sensibili per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.
Va evitato:

- lasciare incustoditi i supporti di memorizzazione, anche per breve periodo, poiché gli stessi possono essere rapidamente letti e copiati;
- per ogni supporto di memorizzazione l'esposizione a campo magnetico (come ad esempio il magnete di un altoparlante, il trasformatore di lampade da tavolo ecc.), in quanto i campi dispersi potrebbero danneggiare il contenuto;
- per ogni supporto di memorizzazione l'esposizione ad alta temperatura e/o al sole di un'autovettura chiusa. Qualora debba essere trasportato da un ambiente caldo ad uno freddo, o viceversa, con possibile sbalzo di temperatura significativo, prima dell'utilizzo deve essere lasciato passare un adeguato intervallo di tempo, per permettere all'eventuale condensa di dissolversi.

Provvedere alla formattazione ex novo egli altri supporti di memorizzazione, prima di registrare dati sensibili, patrimoniali, confidenziali, etc.

Proteggere:
- da sovrascritture i supporti di memorizzazione se utilizzati su differenti postazioni di lavoro;
- con apposite buste o contenitori, che ne dimostrino l'effrazione, i supporti di memorizzazione spediti o consegnati a terzi.

Identificare ogni supporto di memorizzazione, per evitare di confonderli.
Custodire personalmente i supporti di memorizzazione che contengono dati personali e patrimoniali.
Accertarsi che il destinatario della eventuale copia del supporto di memorizzazione abbia lo stesso profilo di autorizzazione del mittente.
Concordare con il destinatario le modalità di cifratura o di apertura del supporto di memorizzazione che contenga dati fondamentali per il patrimonio informativo dell'OPI di Vicenza.
Qualora il contenuto della memoria USB debba essere copiato su un hard disk, od altro strumento elettronico di trattamento, accertarsi di cancellare il relativo contenuto al termine dell'operazione di trattamento, in modo che l'asportazione dalla memoria USB comporti l'asportazione completa dei dati registrati, in via temporanea, sullo strumento elettronico. Si presti una particolare attenzione a che nessun dato sia rimasto nella memoria buffer, nella clipboard, negli appunti o all'interno del cestino, in sistemi operativi di tipo Windows.
Per quanto attiene alle limitazioni d'uso circa l'adozione dei supporti di memorizzazione dei dati in ambito lavorativo l'utilizzatore dovrà attenersi alle norme comportamentali indicate nelle Lettere "istruzioni agli autorizzati al trattamento dei dati personali".

2. Altri tipi di supporto di memorizzazione (DVD-CD-ROM)

Nell'ambito della quotidianità d'uso delle tecnologie informatiche potrebbe essere necessario ricorrere all'utilizzo di differenti supporti di memorizzazione quali ad esempio DVD, CD-ROM ecc. Tali supporti, devono essere trattati per evitare l'eventuale recupero dei dati da parte di soggetti non autorizzati o terzi con la conseguente esposizione debitoria, d'immagine e penale.
In particolare, se contenenti dati sensibili, devono essere custoditi in contenitori ovvero in archivi chiusi a chiave ovvero, in assenza, mediante la definizione di idoneo contenitore protetto.
È altresì opportuno:
- evitare di lasciare incustoditi i supporti di memorizzazione, anche per breve periodo, poiché gli stessi possono essere rapidamente letti e copiati;
- identificare ogni supporto di memorizzazione, per evitare di confonderli CD-ROM R+RW;
- proteggere con apposite buste o contenitori, che ne dimostrino l'effrazione, i supporti di

memorizzazione spediti o consegnati a terzi;
- accertarsi che il destinatario della eventuale copia del supporto di memorizzazione abbia lo stesso profilo di autorizzazione del mittente;
- custodire personalmente i supporti di memorizzazione che contengono dati patrimoniali;
- evitare l'esposizione del DVD, CD-ROM etc. ad alta temperatura, al sole di un'autovettura chiusa o con temperatura significativa.
- in caso di alienazione provvedere alla distruzione rigando la superficie per poi spezzarli.

Per quanto attiene alle limitazioni d'uso circa l'uso dei supporti di memorizzazione dei dati in ambito lavorativo l'utilizzatore dovrà attenersi alle norme comportamentali indicate nelle Lettere "Istruzioni agli Autorizzati al trattamento dei dati personali comuni e sensibili".

Articolo 12 - Uso della posta elettronica

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni, per le finalità dell'OPI di Vicenza ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente o collaboratore che utilizza tale funzionalità.
Non è possibile utilizzare tale servizio per finalità in contrasto con quelle della società o non pertinenti all'attività lavorativa.
Al fine di non compromettere la sicurezza dell'OPI di Vicenza e di prevenire conseguenze legali o di altro genere, gli utenti dovranno adottare i seguenti comportamenti:
- se, nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi), evitare di aprirle (in particolare se contenenti allegati .exe o .pdf), e procedere all'inoltro all'Amministratore di Sistema;
- non utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

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.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Articolo 13 - Navigazione in internet

Il 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.
Al fine di evitare la navigazione in siti con contenuti non attinenti all'attività lavorativa, l'OPI di Vicenza rende peraltro nota l'adozione di uno specifico sistema di blocco, o filtro automatico, che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una blacklist (ciò avviene a mezzo Firewall fisico ovvero a mezzo del fornitore del servizio Fibra come TIM SPA).

Regolamento interno per l'uso dei sistemi informatici

Articolo 14 - Protezione antivirus

Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale preposto alla gestione dei Sistemi Informatici.

Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso in cui venga rilevato un virus, dovrà essere prontamente consegnato al personale preposto alla gestione dei Sistemi Informatici.

L'uso di un dispositivo USB di Memoria deve essere comunque autorizzato dall'Amministratore del Sistema per evitare di danneggiare la rete (possibile presenza di Virus).

Si elencano di seguito alcune regole generali di comportamento (legate ad esempio all'uso della Posta Elettronica) che devono essere sempre seguite per ridurre al minimo il rischio di infezioni da virus informatici che comprometterebbero l'integrità del patrimonio informativo:

- evitare di aprire allegati alle E-Mail direttamente dal programma di posta; è preferibile procedere al salvataggio dell'allegato su una cartella locale permettendo così di verificarne l'effettiva "estensione" (un file di testo .TXT potrebbe mascherare un file .TXT.vbs dannoso); alcuni virus/worm si diffondono, infatti, utilizzando una doppia estensione finale; ad esempio il file "pippo.txt.exe" non è un file di testo (.txt), ma un file eseguibile (.exe); un allegato del genere non va mai aperto o salvato, va cancellata immediatamente l'E-Mail e, successivamente, svuotata la cartella "Posta eliminata";
- qualora, senza l'intervento dell'utente, durante l'anteprima dell'E-Mail, appaia una finestra del client di posta che avverte se aprire o salvare l'allegato, annullare la richiesta e cancellare l'E-Mail; alcuni virus/worm sono in grado di "forzare" l'utente ad aprire l'allegato;
- non aprire mai file eseguibili o dal contenuto attivo (con estensione .exe, .pif, .com, .vbs, .bat, .cmd, .dot, .reg, .js, .scr, .xlm, .wmz, .jar, .html, excel con macro);
- non fare eccezioni anche se il mittente è una persona conosciuta e fidata in quanto, a volte, i virus si "impossessano" della casella E-Mail e/o della rubrica di un utente e inviano E-Mail infette in maniera "autonoma"; a volte i virus sono in grado di falsificare anche il mittente dell'E-Mail, pertanto si potrebbero ricevere E-Mail da falsi sistemi automatici antivirus che ci informano di essere infetti; nella maggior parte dei casi si tratta di un falso allarme; in tale circostanza è opportuno verificare che l'antivirus sia correttamente funzionante;
- diffidare sempre delle E-Mail inviate da mittenti sconosciuti o che inviano allegati non attesi o da offerte gratuite di software, immagini, password di accesso a siti, o altri beni;
- limitare l'iscrizione a forum, newsgroup e liste di distribuzione pubbliche, in modo da non diffondere, ove non necessario, il proprio indirizzo E-Mail (utilizzare pertanto lo strumento elettronico in conformità con quanto indicato nelle lettere di incarico al trattamento dei dati); tale raccomandazione è anche una valida strategia di difesa contro il fenomeno dello "spamming", cioè l'invio massivo di E-Mail pubblicitarie o dai contenuti offensivi e illegali.

Regolamento interno per l'uso dei sistemi informatici

Articolo 15 - Utilizzo dei telefoni e fotocopiatrici
Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, e quindi non sono consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa, salvo espressa autorizzazione da parte della Direzione.
È vietato l'utilizzo delle fotocopiatrici per fini personali, salva preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

Articolo 16 - Accesso ai dati trattati dall'utente
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione, accedere direttamente, nel rispetto della normativa sulla privacy e dei diritti dei lavoratori, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico generato.

Articolo 17 - Accesso remoto alla rete informatica (assistenza) e condivisione Schermo (web meeting)
L'accesso remoto alla rete informatica (esempio Teamviewer, Logmein, VNC, ecc.) è generalmente vietato salvo espressa autorizzazione da parte dell'amministratore delle reti che ne valuta la fattibilità e la pertinenza.
Diverso è il caso d'uso di sistemi di conferenza remota (Meet, Teams, Cisco ecc) che consentono di condividere lo schermo ma ciò soggiace alla reciproca informativa di liceità ed è funzionale a proseguire le attività lavorative.

Articolo 18 - Manutenzione della rete informatica
Durante la pausa pranzo si possono verificare delle interruzioni dei servizi di rete funzionali alla manutenzione dell'infrastruttura stessa. Per tale motivo devono essere chiuse tutte le applicazioni e finestre attive prima di lasciare la propria postazione.

Articolo 19 - Modalità di segnalazione delle criticità
Qualora gli utenti riscontrino problemi di qualsiasi tipo possono inoltrare una richiesta di assistenza al personale interno preposto al contatto con l'amministratore delle reti inoltrando una E-Mail a vicenzaopi@opivicenza.it

Articolo 20 - Sistemi di controlli graduali
In caso di anomalie, il personale incaricato effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.
Le dotazioni di cui al presente Regolamento sono strumenti di lavoro e, pertanto, rientrano nella disciplina dell'art.23 comma 2 del Decreto legislativo n. 151/2015. Il datore di lavoro può, se del caso, effettuare controlli per la verifica dei volumi di traffico sviluppati dal dipendente nell'arco

orario della prestazione lavorativa, per monitorare il corretto utilizzo dello strumento e perseguire eventuali condotte illecite e/o lesive dell'interesse dell'OPI di Vicenza.
Le attività di controllo saranno effettuate a cura dei settori preposti alla tutela del patrimonio e della sicurezza.

Articolo 21 - Disposizioni di carattere generale
I collaboratori dell'OPI di Vicenza possono introdurre e tenere con sé dispositivi elettronici personali, come telefoni cellulari, durante l'orario di servizio. L'utilizzo di tali dispositivi è consentito esclusivamente per esigenze connesse all'attività lavorativa o per urgenti necessità di carattere personale, nel rispetto delle proprie mansioni e senza arrecare pregiudizio allo svolgimento del lavoro.
Resta inteso che l'uso improprio o eccessivo dei dispositivi, tale da configurare una distrazione indebita o un potenziale rischio per la sicurezza nei luoghi di lavoro, potrà essere oggetto di valutazione e richiamo.
L'OPI di Vicenza declina ogni responsabilità in caso di smarrimento, furto o danneggiamento dei dispositivi elettronici personali introdotti nei locali della sede. La responsabilità per l'uso corretto e appropriato di tali dispositivi ricade integralmente sul singolo collaboratore.

Articolo 22 - Furto e smarrimento
In caso di furto o smarrimento del PC Portatile e/o delle dotazioni, l'assegnatario ha l'obbligo di effettuare tempestiva segnalazione all'Amministratore di sistema. La segnalazione dovrà essere corredata della copia della denuncia presentata alle competenti autorità di Pubblica Sicurezza completa di tutte le informazioni relative a marca, tipo e numero matricola identificativo del PC Portatile e del tablet.
È facoltà dell'OPI di Vicenza procedere alla reintegrazione del PC Portatile e/o degli accessori e del tablet (eventuale). L'eventuale reintegro, in caso di furto e/o distruzione incolpevole, è a carico dell'OPI di Vicenza.

Articolo 23 - Manutenzione della dotazione
La manutenzione della dotazione (Pc, Pc Portatile, Tablet) viene garantita dall'OPI di Vicenza, salvo i casi in cui il guasto sia determinato da cattivo uso o danneggiamento imputabile al dipendente assegnatario.
La manutenzione prevede la sostituzione contestuale della dotazione di servizio non funzionante con dotazione sostitutiva quando disponibile.

Articolo 24 - Restituzione dei beni
Al momento della cessazione del rapporto di lavoro, per qualsiasi causa intervenuta, l'assegnatario è tenuto alla immediata restituzione all'Ufficio IT (amministrazione di sistema), o all'ufficio del personale, del bene assegnato in comodato compresi eventuali accessori.
La restituzione è prevista anche nel caso in cui il dipendente si assenti per un periodo di tempo prolungato (con o senza corresponsione della retribuzione), mantenendo il diritto alla conservazione del posto di lavoro, salvo diversi accordi.

Articolo 25 - 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 e Modello Organizzativo interno, nonché con tutte le azioni civili e penali consentite.

Articolo 26 - Trattamento dei dati personali informativa ai sensi del Reg. UE 679/2016 ed ai sensi dell'art.4, comma 3, L.300/1970.

L'OPI di Vicenza tratterà i dati personali del dipendente per le finalità connesse alla gestione della Rete con le modalità espresse nello stesso Regolamento.

I dati personali verranno impiegati per fini relativi alla gestione del rapporto di lavoro ai sensi di quanto previsto dall'art. 4, comma 3, della L. 300/1970, come sostituito dall'art. 23 D.Lgs.151/2015.

Per quanto non espressamente previsto nel presente Regolamento si rinvia all'informativa già in possesso del singolo dipendente.

Articolo 27 - Entrata in vigore

Il presente Regolamento entra in vigore il giorno successivo all'approvazione da parte del Comitato Centrale FNOPI.

Regolamento interno per l'uso dei sistemi informatici

ALLEGATI

Allegato 1) Modalità di ripristino dei dati

LE COMPLETE MODALITÀ DI RIPRISTINO DEI DATI SONO REPERIBILI IN APPOSITE PROCEDURE OPERATIVE REDATTE DAL COMPETENTE AMMINISTRATORE DEL SISTEMA.

Presupposti
I salvataggi dei dati avvengono quotidianamente nella settimana lavorativa in modo automatizzato.
I dati salvati sono archiviati in prima battuta su disco e poi, settimanalmente, su nastro disco esterno. Le modalità sono dichiarate nella procedura operativa qui sopra citata.
La procedura di ripristino è gestita centralmente dal CED su richiesta dell'utente.
I dati che vengono sottoposti a salvataggio riguardano tutte le unità di rete mappate per i vari profili utente. Non sono altresì sottoposti a salvataggio i singoli PC assegnati agli utenti e al Segretario istituzionale.

Cosa si deve fare per richiedere un Ripristino
Per richiedere la procedura di ripristino si deve inviare una richiesta via e-mail all'indirizzo di supporto rsilvestrin@atsservice.it indicando:

- il percorso completo del (o dei) file, o della cartella da ripristinare;
- il nome esatto del (o dei) file, o della cartella;
- l'ultima data valida di ripristino;
- il percorso e il nome del file ripristinato (potrebbe essere l'originale o diverso).

Termine del processo di restore
Il CED provvederà ad avvisare l'utente richiedente del termine del processo di ripristino o a contattarlo in caso di dubbi o problematiche sorte durante il processo stesso.