Regione del Veneto
Istituto Oncologico Veneto
IRCCS

DIREZIONE GENERALE			
REGOLAMENTO			
REGOLAMENTO CONCERNENTE L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI			
		pag. 1	di 21
Codice	I_DG_R58		
Revisione	00		
Data approvazione	30/12/2024		
Data entrata in vigore	Si rimanda all'adozione della relativa Deliberazione del Direttore Generale		
Iniziativa	Direttore f.f. UOC Sistemi Informativi – Andrea Longo		
Redazione	Gruppo di lavoro coordinato dal Direttore f.f. UOC Sistemi Informativi – Andrea Longo		
Verifica	Direttore Scientifico – Vincenzo Bronte Direttore Sanitario – Anna Maria Saieva Direttore Amministrativo – Fabrizio Garbin		
Approvazione	Direttore Generale – Maria Giuseppina Bonavina		
Distribuzione	Direttori/Responsabili		
Responsabile di processo	UOC Sistemi Informativi		
Parole chiave	Regolamento, utilizzo, sistemi, informatici		
Requisiti/Standard	GEN.SAN.AU.ACC.	IRCCS	
	1.4.1	Sez. F, 1-5	

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Sommario

Art. 1. Scopo e campo di applicazione ... 3
Art. 2. Riferimenti ... 4
Art. 3. Riepilogo delle revisioni ... 4
Art. 4. Termini, definizioni e abbreviazioni ... 4
Art. 5. Modalità operative – Disposizioni per l'utilizzo dei sistemi informatici ... 5
Art. 5.1. Modalità operative – Disposizioni per l'utilizzo dei sistemi informatici ... 5
Art. 5.1.1. Gestione delle modifiche ... 7
Art. 5.1.2. Proroga delle credenziali per l'utilizzo dei sistemi informatici ... 7
Art. 5.1.3. Creazione, custodia e utilizzo delle credenziali ... 8
Art. 5.2. Servizio Help Desk ... 8
Art. 5.3. Utilizzo della rete internet ... 8
Art. 5.4. Cartelle di rete ... 9
Art. 5.5. Utilizzo del personal computer (postazione fissa) ... 10
Art. 5.6. Utilizzo dei dispositivi mobili ... 10
Art. 5.6.1. Telefono aziendale ... 11
Art. 5.7. Utilizzo e conservazione dei supporti rimovibili ... 12
Art. 5.8. Utilizzo fax, scanner e fotocopiatrici aziendali ... 12
Art. 5.9. Interventi di manutenzione sul personal computer ... 12
Art. 5.10. Protezione antivirus ... 13
Art. 5.11. Smarrimento e furto delle risorse ICT ... 13
Art. 5.12. Acquisizione dei beni informatici hardware e software ... 14
Art. 5.13. Utilizzo applicativi informatici accessibili dalle postazioni di lavoro ... 14
Art. 5.13.1. Utilizzo degli applicativi informatici ... 14
Art. 5.13.2. Accesso applicativi e condivisione dati aziendali con enti terzi per attività clinica e/o ricerca ... 14
Art. 5.13.3. Utilizzo della posta elettronica ... 14
Art. 5.14. Accesso in lavoro a distanza (telelavoro e lavoro agile) ... 17
Art. 5.15. Uso dei social network ... 17
Art. 5.15.1. Utilizzo di chatbot o altri sistemi basati su intelligenza artificiale ... 18
Art. 5.16. Dati aziendali ... 18
Art. 5.16.1. Esportazione dati ... 19
Art. 5.16.2. Conservazione e archiviazione informatica dei dati ... 19
Art. 5.16.3. Archiviazione e trasmissione informatica di dati particolari ... 19
Art. 5.17. Gestione degli incidenti e Data Breach ... 20
Art. 5.18. Osservanza delle disposizioni in materia di privacy ... 20

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Art. 5.19. Accesso ai dati trattati dall'utente 20
Art. 5.20. Sistema di controlli graduali 20
Art. 5.21. Sanzioni 21
Art. 5.22. Norma di rinvio 21
Art. 5.23. Entrata in vigore 21

Art. 1. Scopo e campo di applicazione

Scopo del Regolamento è disciplinare l'utilizzo delle risorse informatiche dell'Istituto Oncologico Veneto IRCCS, tenuto conto che l'utilizzo di tecnologie informatiche e telefoniche ha consentito l'introduzione di innovative tecniche di gestione delle attività, dando però origine a numerose problematiche circa il loro utilizzo durante lo svolgimento delle mansioni lavorative. Si vuole dunque regolamentare l'utilizzo dei sistemi forniti dall'Istituto tenendo conto:

- delle implicazioni in termini di sicurezza, disponibilità ed integrità dei sistemi informatici dell'ente;
- della prevenzione di comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza di sistemi aziendali e nel trattamento dei dati;
- dell'utilizzo delle risorse informatiche e telematiche che deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro;
- della necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte degli operatori nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 1.3.2007) nonché di quanto stabilito dalla Legge 300/1970 (Statuto dei Lavoratori) e di valutare conseguentemente gli usi scorretti che, oltre a esporre l'Istituto stesso a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile;
- del fatto che i controlli sull'uso degli strumenti informatici e telefonici devono garantire sia il diritto dell'Ente di proteggere la propria organizzazione, sia il diritto del lavoratore a non vedere invasa la propria sfera personale. I computer, gli applicativi per la gestione delle diverse attività, i telefoni aziendali e gli altri mezzi sono strumenti di lavoro, il cui utilizzo personale è precluso, fatto salvo il diritto alla riservatezza ed alla dignità come previsto dalla normativa vigente;
- dell'informazione degli interessati sulle finalità dell'utilizzo degli strumenti informatici, del controllo e sulle specifiche metodologie adottate per effettuarlo;
- della sensibilizzazione degli interessati al rispetto della normativa sulla tutela legale del software;
- che l'utilizzo delle risorse e dei servizi informatici e di rete è subordinato al rispetto da parte degli operatori delle norme civili, penali e amministrative applicabili.

Il presente Regolamento si applica a tutto il personale senza distinzione di ruolo e/o livello o di inquadramento. Pertanto, tutti coloro che svolgono attività professionale, formativa o di volontariato presso lo IOV-IRCCS sono tenuti al rispetto di quanto prescritto nel presente Regolamento.

Riferimenti Gruppo di Lavoro:

Componente	Unità Operativa	Funzione
Andrea Longo	Sistemi Informativi	Revisione documentale
Federico Altieri	Sistemi Informativi	Redazione documentale
Matteo Persona	Sistemi Informativi	Redazione documentale

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Giulia Volpato	Sistemi Informativi	Redazione documentale
Antonio Sciuto	Affari Generali - ufficio Privacy	Redazione area Privacy

Art. 2. Riferimenti

Normativa nazionale/regionale	GDPR 679/2016 Legge 300/1970 (Statuto dei Lavoratori)
Requisiti/standard	GEN.SAN.AU.ACC. 1.4.1 – Presenza nelle strutture sanitarie di sistemi informativi che consentano la tracciatura dei dati sanitari e forniscano il supporto alle attività di pianificazione e controllo che tengano conto anche del debito informativo verso il Ministero della Salute (NSIS). Tali sistemi devono garantire sicurezza nell'accesso e nella tenuta dei dati, ivi compresa la loro integrità, nel rispetto e in ottemperanza alla legislazione e alla normativa vigente in materia.
	IRCCS sez. F, 1-5 – Digitalizzazione delle attività assistenziali; Presenza banda larga; Apparecchiature per videoconferenza compatibili con la rete associativa; Tipo di applicazioni presenti in rete; Numero e tipologia servizi offerti in rete (escluso CUP)

Art. 3. Riepilogo delle revisioni

Revisione	Data approvazione	Oggetto della revisione
00	30/12/2024	Prima approvazione

Art. 4. Termini, definizioni e abbreviazioni

Utente: è la persona autorizzata ad accedere alla rete informatica, alla posta elettronica, agli applicativi, e alle altre risorse informatiche e telematiche messe a disposizione dall'azienda.

Matricola: è il numero assegnato ad inizio del rapporto lavorativo con l'azienda.

Userid: è il numero assegnato ad inizio del rapporto lavorativo con l'azienda ed inizia con una lettera che identifica la tipologia di contratto. (es. t = contratto ind. e det., k = contratti atipici, c = specializzandi, …).

Titolare del trattamento: si intende una qualsiasi persona fisica o giuridica coinvolta nella determinazione delle finalità e delle modalità del trattamento dei dati personali.

Responsabile del trattamento: si intende una qualsiasi persona fisica o giuridica coinvolta nel trattamento dei dati personali degli utenti per conto del titolare del trattamento.

Autorizzato al trattamento: è la persona fisica autorizzata a compiere operazioni di trattamento dati dal titolare del trattamento.

Dati personali: nel contesto del GDPR si riferiscono a tutti i dati relativi a una persona vivente identificata o identificabile. Sono incluse anche informazioni che, se raccolte insieme, possono portare all'identificazione. Ciò vale anche per i dati crittografati o presentati con l'uso di pseudonimi, finché la crittografia/anonimizzazione è reversibile.

Dati sensibili: sono categorie speciali di informazioni personali, che devono essere trattate con maggiore attenzione dall'incaricato del trattamento/autorizzato al trattamento in quanto a differenza dei normali dati personali, i dati sensibili potrebbero potenzialmente portare alla discriminazione dell'utente, se condivisi. Tra le categorie speciali di dati personali, il GDPR include: l'origine razziale o etnica; le opinioni politiche; le convinzioni religiose o filosofiche; l'appartenenza a sindacati; i dati genetici; i dati biometrici (la biometria è

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

una misurazione umana che può portare all'identificazione di una persona. Si tratta di dati come le impronte digitali, il riconoscimento facciale, il DNA, ecc.); dati relativi alla salute; dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.
E-mail: indica la funzione di posta elettronica per lo scambio di messaggi e di documenti.
Download: è l'azione di ricevere o prelevare dalla rete informatica un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente.
Upload: è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica.
Freeware: è un software che viene distribuito in modo gratuito.
Shareware: è un software che può essere liberamente ridistribuito, e può essere utilizzato per un periodo di tempo di prova variabile, scaduto il quale, per continuare ad utilizzare il software è necessario registrarlo presso la casa produttrice, pagandone l'importo.
Ransomware: è un tipo di malware che limita l'utilizzo del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione.
Dominio: rete privata di computer avente determinate logiche di gestione e regole applicate ad ogni dispositivo connesso in rete.
Spyware: è un tipo di malware che raccoglie informazioni e/o monitora l'attività dell'utente (memorizzazione tasti premuti, credenziali di autenticazione, …) senza il suo consenso, trasmettendole su server remoti per utilizzarle per attività dannose sfruttando i contenuti ad esse associate.
Phishing: è un tipo di truffa effettuata tramite messaggi o email dove l'attaccante cerca di portare l'utente finale ad aprire un link, dal quale poi verrà scaricato un malware, oppure semplicemente ad inserire credenziali/informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile (anche simulando una mail aziendale) in una comunicazione digitale.
Malware: abbreviazione per malicious software o "software malevolo". È un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema, cercando di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo.
Data breach o violazione dei dati personali: l'incidente di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Cloud: infrastruttura tecnologica che mette a disposizione capacità computazionale e/o spazio di archiviazione. I fornitori di servizio cloud vendono la suddetta capacità computazionale e/o lo spazio di archiviazione sotto forma di servizio a sottoscrizione.
Servizio in cloud: servizio erogato sfruttando una piattaforma cloud.
VDI: Virtual Desktop Infrastructure, virtualizzazione del proprio desktop aziendale, utilizzato per l'accesso dell'utente da remoto.
Cartelle di rete condivise: sono cartelle di rete condivise nei server dell'Istituto all'interno del dominio aziendale.
Servizi di storaging aziendali: si intendono sia i server in rete aziendale atti alla archiviazione e condivisione di file tra dipendenti per collaborare in maniera efficace che servizi di archiviazione in cloud.

Art. 5. Modalità operative – Disposizioni per l'utilizzo dei sistemi informatici

Art. 5.1. Modalità operative – Disposizioni per l'utilizzo dei sistemi informatici

L'accesso al dominio e ai sistemi informativi messi a disposizione del personale autorizzato per lo svolgimento delle mansioni assegnate avviene mediante l'inserimento delle credenziali di autenticazione al dominio, cioè lo userid e la password. Lo userid è composto da una lettera iniziale e il numero di matricola, invece la password viene impostata dall'utente, seguendo il link e le istruzioni inviate tramite e-mail. L'utente è tenuto

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

a effettuare il cambio password periodicamente, almeno ogni tre mesi.
Le credenziali vengono attribuite secondo il criterio del minimo privilegio in base al quale ogni utente deve avere credenziali atte a permettere l'accesso e l'uso solo per le risorse informatiche strettamente necessarie a svolgere le mansioni assegnate. I privilegi di accesso alle risorse informatiche garantiti dalle credenziali vengono definiti in base al principio della stretta pertinenza e necessità per l'utente.
Le credenziali vengono concesse esclusivamente per lo svolgimento delle attività previste nell'ambito del rapporto di lavoro/collaborazione con IOV-IRCCS. La gestione delle credenziali deve essere effettuata nel pieno rispetto della normativa privacy vigente.
La creazione dell'utenza a dominio ("Account") con la definizione dello userid per i dipendenti e per tutto il personale registrato nell'applicativo software di gestione delle risorse umane avviene-all'atto di assunzione.
Le credenziali di accesso al dominio aziendale, agli applicativi ad esso collegati, alle risorse in rete (dischi, stampanti, etc.) e alla posta elettronica dello IOV-IRCCS – sia nominativa che di gruppo - vengono concesse esclusivamente per lo svolgimento dell'attività professionale. Conseguentemente, le relative abilitazioni agli utenti sono determinate dall'inquadramento e dalle mansioni attribuite a ciascun utente e dalle richieste avanzate dal Responsabile dell'utente o comunque da soggetto titolato ad effettuare tale richiesta (nel seguito "Referente") o suo delegato (nel seguito "Delegato").
Le richieste di attribuzione di credenziali devono essere indirizzate ai Sistemi Informativi con le modalità di volta in volta definite in apposita Istruzione Operativa. Le richieste devono essere effettuate con l'approvazione del Responsabile/Referente/Delegato dell'utente.
In caso di personale non dipendente (es. collaboratori con propria Partita IVA) o di altri soggetti esterni la suddetta richiesta deve essere effettuata dal Referente/Delegato IOV interessato alla collaborazione con l'utente. Tale richiesta deve precisare l'intervallo temporale per cui si chiede il perdurare delle credenziali ed essere corredata di adeguata documentazione che ne attesti il rapporto contrattuale o di collaborazione.
I Sistemi Informativi curano l'attribuzione dei conseguenti privilegi associati alle credenziali per quasi tutte le risorse informatiche interessate; in alcuni casi le credenziali vengono rilasciate e gestite da specifici servizi (es. per HR Sigma la gestione è in carico alle Gestione Risorse Umane e per SGP il Servizio Gestione Agende).
Per quanto riguarda applicativi software o altre risorse non collegate al dominio aziendale, le richieste di attribuzione di credenziali avvengono con le stesse modalità sopra descritte. In aggiunta, nella richiesta di abilitazione deve essere precisato per ogni applicativo a cui si chiede l'accesso quanto segue:

- modalità di accesso all'applicativo (solo visualizzazione, modifica, cancellazione, etc.);
- motivazione per l'accesso all'applicativo (es. motivazione per cui un soggetto esterno quale un fornitore necessità di accedere ad un applicativo).

Nel caso si renda necessario per un utente accedere a risorse fisiche ad accesso ristretto (es. supporti di memorizzazione, dispositivi non collegati in rete aziendale dello IOV-IRCCS), le richieste di attribuzione di credenziali avvengono con le stesse modalità sopra descritte. In ogni richiesta deve essere indicata la motivazione che la origina.
Per alcune categorie di collaboratori dello IOV-IRCCS potrebbe essere esclusa l'abilitazione ad accedere alle risorse collegate al dominio aziendale. Pertanto:

- i tirocinanti a scopo di orientamento, gli studenti che frequentano lo IOV-IRCCS per l'alternanza scuola-lavoro, così come i frequentatori volontari non sono autorizzati ad accedere alle risorse informatiche dello IOV-IRCCS né alla posta elettronica;
- i tirocinanti pre e post lauream sono abilitati ad accedere agli applicativi necessari alle attività formative solo per visualizzare i dati. Non è previsto l'utilizzo di un account di posta istituzionale;
- i tirocinanti che accedono allo IOV-IRCCS per ottenere l'abilitazione alla professione ottengono abilitazioni coerenti con il profilo professionale;
- i frequentatori volontari intesi come coloro che accedono allo IOV-IRCCS ai fini formativi e di aggiornamento per acquisire, approfondire o perfezionare le conoscenze relativi ad attività svolte presso l'Istituto, non possono accedere alle risorse informatiche aziendali né alla posta elettronica;
- come specificato all'art. 34 del Regolamento per le scuole di specializzazione di area sanitaria adottato

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

dall'Università degli Studi di Padova (decreto 4208/2019) che prevede almeno tre livelli di autonomia dello specializzando, i medici specializzandi possono accedere agli applicativi aziendali distinguendo le seguenti tre casistiche:

1. "*attività assistenziale "senza autonomia": il medico in formazione specialistica è direttamente coinvolto nelle attività assistenziali, negli atti medici e nelle decisioni cliniche, sempre con supervisione diretta da parte del medico strutturato presente*".
   Tali specializzandi hanno accesso agli applicativi con le stesse autorizzazioni dei medici, ma non hanno firma digitale e non emettono ricette;
2. *"attività assistenziale "in autonomia tutorata": il medico in formazione specialistica può eseguire attività assistenziali, atti medici e prendere decisioni cliniche in autonomia, potendo ricorrere alla supervisione immediata del medico strutturato presente".*
   Tali specializzandi hanno accesso agli applicativi con le stesse autorizzazioni dei medici, ma non hanno firma digitale e non emettono ricette;
3. *"attività assistenziale "in autonomia": il medico in formazione specialistica può eseguire attività assistenziali, atti medici e prendere decisioni cliniche in autonomia, potendo, a proprio giudizio, ricorrere al medico strutturato presente".*
   Tali specializzandi hanno accesso agli applicativi con le stesse autorizzazioni dei medici, hanno firma digitale e sono autorizzati ad emettere ricette e prescrizioni.

Art. 5.1.1. Gestione delle modifiche

In ogni situazione in cui, per qualsiasi motivo (attribuzione di mansione diversa, cambiamento di struttura organizzativa di appartenenza, cambiamento di ruolo in caso di soggetto esterno) cambino le risorse informatiche a cui l'utente necessita di accedere, ai Sistemi Informativi deve pervenire, tramite i canali formali definiti da apposita Istruzione Operativa vigente, una comunicazione dell'avvenuto cambiamento inviata dal Responsabile/Referente/Delegato dell'utente, integrata, ove applicabile, dalla richiesta di accesso a differenti risorse informatiche.
I Sistemi Informativi si fanno carico di rimuovere i privilegi assegnati in precedenza e di attivare nuovi privilegi conseguenti alla richiesta.
La richiesta di sospensione delle credenziali per un certo intervallo temporale può essere inviata Responsabile/Referente/Delegato dell'utente ai Sistemi Informativi con allegata descrizione delle motivazioni.
I Sistemi Informativi prendono in carico la richiesta sospendendo temporaneamente il possibile utilizzo delle credenziali. La riattivazione delle credenziali viene effettuata dai Sistemi Informativi solo a seguito di speculare richiesta da parte del Responsabile/Referente/Delegato dell'utente.
In caso di inutilizzo per un periodo superiore a 6 mesi i Sistemi Informativi valutano se disabilitare le credenziali.
In caso di cessazione, per qualsiasi motivo, del rapporto di lavoro/collaborazione con lo IOV-IRCCS, ai Sistemi Informativi deve pervenire, tramite i canali formali definiti da apposita Istruzione Operativa vigente, una comunicazione, inviata dalle Risorse Umane, dell'avvenuta cessazione,
I Sistemi Informativi si fanno carico di disattivare le credenziali e di procedere con tutti gli adempimenti necessari per garantire il corretto funzionamento delle risorse informatiche interessate.

Art. 5.1.2. Proroga delle credenziali per l'utilizzo dei sistemi informatici

Nel momento in cui l'utenza non ha più un rapporto di lavoro o collaborazione con IOV, non sarà possibile prorogare l'utenza di dominio e la mail aziendale, quindi l'utente non potrà più avere accesso alle risorse istituzionali.
Sarà possibile prorogare l'utenza solo nel caso in cui l'utente sia in attesa del rinnovo del contratto, per un periodo di tempo pari ai tempi tecnici necessari a tale rinnovo.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Art. 5.1.3. Creazione, custodia e utilizzo delle credenziali

Per effettuare il primo accesso al dominio aziendale, viene inviata al nuovo utente una mail (all'indirizzo personale) contenente un link per impostare la password, con le istruzioni da seguire. Tale password deve essere modificata con cadenza trimestrale.
Le password utilizzate per l'accesso alle risorse informatiche devono essere cambiate a cura degli utenti seguendo le modalità e tempistiche specificamente determinate per tali risorse.
La password non deve contenere riferimenti riconducibili al titolare della stessa (esempio: riferimenti al codice fiscale, al proprio nome/cognome o quello di un familiare o amico stretto, etc.) e come da suggerimenti del Garante sulla creazione delle password deve essere generata preferibilmente senza un significato compiuto; nello scegliere la propria password devono essere utilizzati anche caratteri speciali secondo quanto permesso dalla risorsa informatica, lettere maiuscole e minuscole, numeri; essa deve essere lunga almeno 12 caratteri.
Le credenziali devono, inoltre, essere custodite con la massima attenzione e segretezza e non devono essere divulgate o comunicate a terzi, siano essi personale dello IOV-IRCCS o soggetti estranei all'Istituto stesso.
Non è consentito l'utilizzo condiviso del proprio account utente, fatte salve le eccezioni esplicitamente autorizzate.
Non usare mai il proprio userid e la propria password per accedere a sistemi esterni se non espressamente autorizzati da indicazioni e procedure aziendali. È vietato utilizzare le credenziali aziendali per fini personali (ad es. per registrarsi a siti web o a servizi usati a titolo personale)
Il titolare delle credenziali è responsabile di ogni utilizzo indebito o non consentito delle stesse.
In caso di perdita di riservatezza della password o sospetto di divulgazione impropria, è necessario effettuare un cambio della password quanto prima possibile. Nel caso in cui si riscontrino problematiche durante la procedura di cambio password, l'utente potrà avere assistenza contattando il servizio di Help Desk aziendale.

Art. 5.2. Servizio Help Desk

Per supportare gli utenti nella gestione e risoluzione di problematiche tecniche relative all'utilizzo delle risorse informatiche aziendali, è attivo il servizio Help Desk dedicato. Si precisa che il supporto dei Sistemi Informativi non copre richieste relative all'utilizzo di sistemi ed applicativi di impiego comune (es: utilizzo Word/Excel) o per cui è stato ricevuto specifico addestramento/formazione (es: Eusis, Archiflow ecc.).
Il servizio Help Desk può essere contattato tramite i canali di seguito riportati:

- Portale Help Desk aziendale: ticket.iov.veneto.it
- E-mail: helpdesk@iov.veneto.it
- Numero di telefono: 049 821 8555

Altre modalità di segnalazione/richieste pervenute tramite canali differenti (es: telefonate ed e-mail a contatti individuali) non saranno prese in carico.
Le modalità di interazione con Help Desk e le tempistiche con cui esso opera sono precisate in apposita Istruzione Operativa.

Art. 5.3. Utilizzo della rete internet

I dispositivi assegnati al singolo utente e abilitati alla navigazione in internet costituiscono uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È vietata la navigazione in internet per attività non lavorative, salvo in caso di necessità e urgenza come previsto dal "DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 giugno 2023, n. 81.
L'utente è direttamente e pienamente responsabile dell'uso di internet, delle informazioni che immette, delle modalità con cui opera, dei siti web che visita e delle altre operazioni da lui effettuate.
L'Istituto Oncologico Veneto presso le sedi di Padova, Schiavonia e di Castelfranco Veneto, si avvale di alcuni servizi di gestione/monitoraggio del servizio, nel rispetto della normativa privacy e nei limiti stabiliti dalla L. 300/1970 (Statuto dei Lavoratori).
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, viene adottato uno specifico sistema di url filtering per prevenire determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

black list. L'Istituto individua categorie di siti considerati correlati con la prestazione lavorativa e compatibili con le finalità istituzionali consentendone l'accesso.
A titolo esemplificativo l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web in particolare se con protocollo http, a meno che non siano strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal responsabile della funzione/Unità organizzativa e/o dei Sistemi Informativi e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- l'iscrizione e la partecipazione a forum o social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal responsabile della funzione/Unità organizzativa.

Solo in caso di segnalazioni o sospetti fondati di violazione della sicurezza aziendale o di richieste provenienti dalle autorità competenti il personale incaricato dai Sistemi Informativi è autorizzato ad effettuare controlli mediante un sistema di monitoraggio dei contenuti (Proxy server) o mediante la consultazione di "file di log" della navigazione. Tali sistemi sono configurati al fine di avere una profondità storica differenziata in relazione alla criticità del dato trattato. In taluni casi (es: cartella clinica del paziente) i "file di log" non vengono mai eliminati.
È vietato tentare di violare o aggirare i sistemi di controllo o di protezione dell'uso di internet e della posta elettronica installati e utilizzati dall'Istituto, nel rispetto del diritto alla riservatezza dei dipendenti.
È, infine, vietato installare e/o utilizzare in modo fraudolento strumenti concepiti per compromettere la sicurezza ed il corretto funzionamento dei sistemi aziendali e/o di terzi.
È vietato monitorare ciò che transita nella rete informatica dell'Istituto, se non espressamente autorizzati dai Sistemi Informativi.

Art. 5.4. Cartelle di rete

Le cartelle di rete condivise non associate a una specifica Unità Operativa presenti nei server dell'Istituto sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere allocato, nemmeno temporaneamente, in queste Unità.
Le cartelle di rete sono associate alle Unità Operative e ai singoli lavoratori competenti ad accedervi. Gli accessi alle cartelle di rete sono profilati per verificare che ad esse accedano i soggetti autorizzati in base al profilo professionale. Alcune cartelle di rete potrebbero essere allocate presso un servizio cloud certificato e autorizzato. Gli spazi cloud sono legati alla propria utenza e/o all'email aziendale, essendo così accessibili da qualunque dispositivo. L'utente è considerato responsabile dei danni derivanti da accessi impropri a spazi cloud aziendali (data breach, perdita di dati) dovuti a imperizia o dolo.
Non è concesso l'utilizzo delle cartelle condivise per spostamento e/o condivisione di file contenenti dati relativi ai pazienti (referti, immagini diagnostiche, …) se non espressamente autorizzato per motivi legati a studi e/o sperimentazioni, per maggior dettaglio si rimanda all'Art. 5.16.2 "Conservazione e archiviazione informatica dei dati".
Il personale incaricato del servizio di assistenza sui sistemi hardware e software in uso presso lo IOV- IRCCS è autorizzato in qualunque momento a procedere alla rimozione di ogni file o applicazione pericolosa o non autorizzata da suddette cartelle. Vengono svolte attività di controllo a campione, di amministrazione e backup da parte del personale incaricato sulla base delle policy di sicurezza informatica di questo istituto.
È compito di ciascun utente, per quanto di propria competenza e secondo i canoni della diligenza, preservare i dati e informazioni aziendali da soggetti terzi non regolarmente autorizzati.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Art. 5.5. Utilizzo del personal computer (postazione fissa)

Il personal computer affidato all'utente è uno strumento di lavoro, quindi ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza aziendale. Essendo che da DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 giugno 2023, n. 81 all'Art.1 comma 4 è consentito quanto segue: *"[...] 4. Al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché' l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali. […]"* si chiede all'utente, una volta assolte le incombenze personali, di eliminare gli eventuali dati personali salvati localmente e di porre la massima attenzione al fine di non cadere in tentativi di phishing. Qualora si abbia il minimo sospetto di essere incappati in una situazione non sicura si chiede all'utente di avvisare i Sistemi Informativi che procederà ad effettuare le verifiche necessarie per garantire la sicurezza aziendale.

Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento, di sottrazione o di accesso indebito/non autorizzato ai contenuti archiviati sul dispositivo stesso. Per proteggersi da accessi non autorizzati, è necessario spegnere il computer prima di lasciare l'ufficio e ogni volta che questo non viene utilizzato. Invece, nel momento in cui ci si deve allontanare dalla propria postazione di lavoro anche per qualche minuto, è necessario attivare il blocco con richiesta password tramite i seguenti comandi: **+ L.** Questa azione deve essere fatta per prevenire l'uso improprio da parte di terzi del computer aziendale, in quanto, essendo connesso alla rete informatica dell'Istituto, può esporre la stessa a un potenziale rischio.

Costituisce buona regola la pulizia periodica (almeno una volta all'anno) delle cartelle, con cancellazione dei file obsoleti o non utili allo svolgimento dell'attività lavorativa. Particolare attenzione deve essere prestata alla duplicazione dei dati evitando l'archiviazione ridondante, specialmente sulle Unità o cartelle di rete condivise.

Durante l'utilizzo del personal computer aziendale non sono permesse le seguenti attività:

- L'archiviazione di dati personali e/o sensibili, dei pazienti o di altri soggetti nei dischi locali del personal computer fornito dall'Istituto. Tali dati dovranno essere archiviati, previa autorizzazione del proprio responsabile, solamente nelle risorse di rete aziendali assegnate all'UO di appartenenza.
- Connettere dispositivi privati (es. cellulari, chiavette usb, ...) al personal computer, salvo specifica richiesta da parte del responsabile di funzione/Unità Operativa e autorizzazione da parte dei Sistemi Informativi.
- Utilizzare programmi diversi da quelli ufficialmente installati dal personale dei Sistemi Informativi per conto dell'Istituto;
- Installare autonomamente programmi, a fronte del grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza di tale disposizione espone sia l'Istituto sia l'utente a gravi responsabilità civili, inoltre le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e non protetto dal diritto d'autore, sono sanzionate penalmente.
- Utilizzare il sistema di comunicazione aziendale per l'accesso a banche dati esterne all'Istituto per attività non inerenti allo svolgimento di mansioni istituzionali.
- Apportare modifiche alle caratteristiche impostate sul proprio personal computer né procedere ad installare dispositivi di memorizzazione (si veda l'Art. 5.7 "Utilizzo e conservazione dei supporti rimovibili"), comunicazione o altro. In caso di necessità legate all'attività lavorativa, deve essere fatta richiesta ai Sistemi Informativi dandone una motivazione.

Non sono consentiti spostamenti di postazioni di lavoro in autonomia; tale richiesta deve pervenire ai Sistemi Informativi tramite interazione con il servizio di Help Desk.

Art. 5.6. Utilizzo dei dispositivi mobili

L'assegnazione al personale di computer portatili, tablet o altri dispositivi (come il telefono aziendale oppure modem wi-fi 4G portatile, comunemente chiamata "saponetta") è preceduta da richiesta trasmessa ai Sistemi Informativi tramite il servizio Help Desk

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

A tutti i dispositivi in dotazione da IOV-IRCCS si applicano tutte le regole previste dal presente Regolamento e gli assegnatari dovranno conservare e custodire tali dispositivi con la massima cura, attenzione e diligenza, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni. In particolare l'utente deve obbligatoriamente impostare un codice di sblocco schermo. Infatti, tali dispositivi possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato, ovvero essere "infettati" da virus o codice malevolo. Peraltro, un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica dell'Istituto, una volta che tali dispositivi siano collegati direttamente alla rete interna.
In caso di dispositivi mobili utilizzati in modo promiscuo da più persone della stessa Unità Operativa la responsabilità dello stesso è in capo al Direttore/Responsabile del servizio o dei suoi delegati.
Qualora l'utente non necessiti più dell'utilizzo del dispositivo mobile, informerà i Sistemi Informativi che si attiverà per la restituzione del dispositivo stesso seguendo la procedura interna. Il personale dei Sistemi Informativi applicherà inoltre le procedure tecniche ed informatiche per l'eliminazione dei file e/o delle configurazioni. L'utente prima della restituzione del dispositivo, si prenderà cura della totale rimozione di eventuali dati personali presenti su di esso.
Tra i diversi dispositivi che IOV-IRCCS dà in dotazione, il computer portatile in particolare è da considerarsi soggetto alle stesse medesime regole della postazione fissa elencate nell'articolo che precede.
In particolare non è consentito connettere i dispositivi aziendali a reti pubbliche, private e/o non sicure, quindi a tutte le reti al di fuori di quella aziendale, se non previa opportuna richiesta motivata da parte del responsabile della Unità Operativa o suo delegato, comunque sempre ai fini di proseguire con l'attività lavorativa. Tale richiesta deve essere approvata dai Sistemi Informativi per le opportune verifiche e il censimento di tali dispositivi per un opportuno monitoraggio. In caso di lavoro a distanza, i dispositivi mobili possono essere collegati alla rete privata del personale che lavora al di fuori delle sedi dell'Istituto.
I dispositivi mobili non devono essere mai lasciati incustoditi e in essi devono essere presenti solo i file strettamente necessari per l'attività lavorativa.
Per motivi di sicurezza, di riservatezza e di integrità dei dati aziendali, è necessario adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito elencate, che gli utenti sono chiamati ad applicare in modo scrupoloso:

- evitare la conservazione di file nei dispositivi, ma conservarli sugli spazi aziendali messi a disposizione;
- collegarsi, con frequenza almeno settimanale, alla rete interna dell'Istituto per scaricare gli aggiornamenti (patch, hot fix, antivirus, …);
- mantenere abilitato l'antivirus;
- non disabilitare le impostazioni di sicurezza originariamente impostate dai Sistemi Informativi;
- accedere e navigare in siti web solo strettamente collegati allo svolgimento delle mansioni professionali, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
- non mantenere abilitati protocolli insicuri di comunicazione, oltre il tempo strettamente necessario (bluetooth, wifi);
- non installare applicazioni o sistemi operativi in modo autonomo. È necessario rivolgersi ai Sistemi Informativi:
- non consentire l'accesso e l'utilizzo del dispositivo se non mediante password, PIN o altra modalità di sblocco/autenticazione.

Art. 5.6.1. Telefono aziendale

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, La ricezione o l'effettuazione di telefonate personali, SMS o MMS è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono aziendale a disposizione.
L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite.
Qualora venisse assegnato un telefono cellulare aziendale all'utente, l'utente stesso sarà responsabile del suo utilizzo e della sua custodia. Valgono per esso, per quanto applicabili, le regole sopra descritte.
Si ricorda che in caso di telefono aziendale utilizzato in modo promiscuo da più persone della stessa Unità Operativa, la responsabilità dello stesso è in capo al Direttore/Responsabile del servizio o dei suoi delegati.

Art. 5.7. Utilizzo e conservazione dei supporti rimovibili

L'archiviazione e la conservazione di documenti, informazioni, dati personali su memorie esterne rimovibili come per esempio: chiavette USB, hard-disk esterni, CD e DVD riscrivibili, etc. è in generale vietata.
In caso di comprovata necessità per lo svolgimento dell'attività lavorativa, i Sistemi Informativi possono assegnare memorie esterne al singolo operatore che ne faccia richiesta e che sia validata dal Direttore/Responsabile di Unità Operativa. Documenti, informazioni, dati personali possono essere archiviati su tali supporti solo per quanto strettamente necessario.
Tutti i supporti rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, SSD ecc.), contenenti dati sensibili nonché informazioni costituenti patrimonio 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. Si fa presente che la semplice cancellazione/eliminazione dei dati dai dispositivi di memorizzazione non preclude il futuro recupero, a meno di non effettuare particolari attività di formattazione a basso livello in carico ai Sistemi Informativi.
Il personale autorizzato all'utilizzo di memorie esterne è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
Al cessare delle esigenze lavorative, il lavoratore per restituire il dispositivo di archiviazione contatta i Sistemi Informativi, che procederanno alla distruzione/cancellazione dei dati e/o dei supporti stessi.
In ogni caso, i supporti rimovibili contenenti dati personali e/o riservati dal punto di vista aziendale, devono essere adeguatamente custoditi dagli utenti, seguendo quanto detto all'Art. 5.6 "Utilizzo dei dispositivi mobili", riponendoliin armadi o cassetti chiusi a chiave presenti presso la sede di lavoro e seguendo, per quanto applicabile, quanto prescritto nel paragrafo "Utilizzo dei dispositivi mobili". Qualora vi fosse la necessità di portarli all'esterno, il lavoratore li dovrà custodire diligentemente osservando le cautele e le misure volte ad evitare la perdita, la sottrazione o l'utilizzo da parte di terzi non autorizzati.
È vietato invece l'utilizzo di supporti rimovibili personali, senza eccezione alcuna.

Art. 5.8. Utilizzo fax, scanner e fotocopiatrici aziendali

Pur essendo ancora in uso, i fax sono in via di dismissione. Si stanno adottando modalità di comunicazione alternativa come posta elettronica e stampa remota.
Nel caso in cui lo scanner e/o stampanti condivisi tra diversi utenti e/o diverse Unità Operative vengano utilizzati per la riproduzione cartacea di documenti contenenti dati sensibili di pazienti o dipendenti, è necessario impostare una stampa in modalità privata. Nel caso in cui questo non fosse possibile si richiede che tali documenti vengano prontamente ritirati. Subito dopo l'utilizzo dello scanner è necessario eliminare i documenti dall'apposita cartella di rete. In caso di permanenza di documenti scansionati nelle cartelle di rete dedicate, il personale dei Sistemi Informativi procederà con attività automatiche di pulizia periodica senza preavviso.
È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.

Art. 5.9. Interventi di manutenzione sul personal computer

Il personale incaricato della manutenzione dei dispositivi hardware e software in uso presso lo IOV-IRCCS è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (quali aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, altro). Gli interventi effettuati per consentire quanto appena specificato potranno comportare l'accesso motivato ai dati e sistemi aziendali (per esempio per prestare assistenza all'utente, eseguire aggiornamenti di software nella sua postazione oppure altre

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

attività che necessitano l'accesso alla postazione di lavoro dell'utente).
Il personale autorizzato incaricato del servizio di assistenza può collegarsi e visualizzare da remoto, previa autorizzazione da parte dell'utente, il desktop delle singole postazioni di personal computer al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, e simili. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e/o telematico. In quest'ultimo caso, fatta salva l'urgenza di procedere per non pregiudicare l'efficacia dell'intervento, verrà data comunicazione all'utente interessato della necessità dello stesso.
Nel personal computer non devono essere presenti file personali, quali ad esempio fotografie, file musicali, file video, file di attività extra lavorative. Durante le operazioni di manutenzione, cambio e/o sostituzione del personal computer (ammodernamento del parco macchine), il tecnico addetto alla sostituzione può rimuovere, se presenti, file non inerenti all'attività lavorativa.
L'Istituto, inoltre, durante queste attività di manutenzione, si riserva di eliminare qualsiasi elemento software la cui installazione sia avvenuta senza formale richiesta da parte del Responsabile/Referente/Delegato di funzione/Unità Operativa e autorizzazione esplicita da parte dei Sistemi Informativi.

Art. 5.10. Protezione antivirus

Il sistema informatico dell'Istituto è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque verificare la presenza dell'antivirus nei propri dispositivi e tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale.
Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni attività in corso, spegnere il personal computer e segnalare prontamente, attraverso gli opportuni canali, l'accaduto al personale del servizio di assistenza dei Sistemi Informativi.
Ogni eventuale supporto di memorizzazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del servizio di assistenza dei Sistemi Informativi.
È importante ricordare che:

- i virus possono alterare o distruggere i dati e i programmi;
- i virus diffusi in internet sono spesso camuffati da programmi di utilità o di intrattenimento;
- ogni computer deve essere protetto da idonei strumenti per il rischio di attività di virus informatici;
- il software antivirus deve essere abilitato ed è vietato disabilitarlo senza l'autorizzazione dei Sistemi Informativi;
- la posta elettronica viene filtrata in entrata da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus. Evitare di aprire messaggi provenienti da mittenti sconosciuti o sospetti. In questo caso è necessario spostare la mail nella sezione "Segnalazione phishing", come già riportato nell'Art. 5.13.3. "Utilizzo della posta elettronica" e avvisare i Sistemi Informativi tramite il servizio Help Desk;
- periodicamente per ogni PC viene controllata la presenza di virus mediante avvio automatico della scansione dell'intero sistema.

Art. 5.11. Smarrimento e furto delle risorse ICT

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto, il lavoratore è tenuto a segnalare tempestivamente l'accaduto al Direttore/Responsabile della propria Unità Operativa di competenza, ai Sistemi Informativi e quando necessario procedere con denuncia presso le autorità di Polizia competenti.
Inoltre si rimanda anche alla procedura aziendale per la gestione dei data breach in quanto lo smarrimento o il furto potrebbero comportare l'accesso illegittimo ai dati personali dei pazienti o dei dipendenti eventualmente contenuti nel dispositivo smarrito o rubato.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Art. 5.12. Acquisizione dei beni informatici hardware e software

L'acquisizione di hardware quale, a titolo esemplificativo, computer fissi, computer portatili, stampanti, scanner, ecc. avviene a seguito di esplicite richieste che devono essere indirizzate ai Sistemi Informativi con le modalità di volta in volta definite in apposita Istruzione Operativa. Le richieste devono essere effettuate con l'approvazione del Responsabile/Referente dell'utente.
I Sistemi Informativi analizzano le richieste pervenute dalle Unità Operative per reperire i dispositivi e i componenti volti a soddisfare le richieste. I Sistemi Informativi effettueranno adeguate analisi per verificare che quanto richiesto sia compatibile con le politiche di gestione e sicurezza del sistema informatico aziendale.
L'approvvigionamento di componenti hardware e software, inclusi componenti non normalmente in dotazione al personale dello IOV-IRCCS, verrà gestito dai Sistemi Informativi con il supporto del Provveditorato nel rispetto della normativa in materia di acquisizione dei beni.
Per garantire che gli applicativi software in uso presso lo IOV-IRCCS rispettino i requisiti tecnici e di sicurezza richiesti e non contrastino con la disciplina in tema di diritto d'autore, non è consentita l'installazione/acquisizione autonoma da parte di Unità Operative o di singoli operatori di tali software.

Art. 5.13. Utilizzo applicativi informatici accessibili dalle postazioni di lavoro

Art. 5.13.1. Utilizzo degli applicativi informatici

Gli applicativi istituzionali sono strumenti di lavoro, quindi il loro utilizzo è consentito previa autenticazione personale e profilazione per le funzioni allo specifico applicativo aziendale. È vietato ogni utilizzo degli applicativi che non sia inerente all'attività lavorativa, con la correlata responsabilità dell'utente in ogni caso di uso illecito.

Art. 5.13.2. Accesso applicativi e condivisione dati aziendali con enti terzi per attività clinica e/o ricerca

Nello svolgimento dell'attività clinica e/o di ricerca può rendersi necessario l'accesso o la condivisione di dati aziendali a terzi o specialisti esterni allo IOV. Si distinguono i seguenti casi:

- Accesso ad applicativi aziendali: l'accesso da parte di esterni ad applicativi aziendali (qualora prevista la possibilità) deve essere richiesto ai Sistemi Informativi da parte della Direzione o del Responsabile di Unità Operativa a cui afferiscono (o suo Delegato) il quale si fa carico di presentare la richiesta e si assume la responsabilità per ogni danno provocato, per dolo o imperizia, dall'utente abilitato.
- Per la condivisione di dati o file si vedano gli Artt. 5.16.2 "Conservazione e archiviazione informatica dei dati" e 5.16.3 "Archiviazione e trasmissione informatica dei dati sensibili".

Si ricorda che nell'apposito modulo di richiesta abilitazione ad uno specifico applicativo e/o servizio è importante ed obbligatorio indicare la data di chiusura del contratto o della collaborazione qualora prevista.

Art. 5.13.3. Utilizzo della posta elettronica

L'Istituto fornisce caselle di posta elettronica associate a ciascuna Unità Operativa, Ufficio o Gruppo di lavoro da utilizzare sia per la corrispondenza interna sia per lo scambio di e-mail con destinatari esterni a fini lavorativi.
Il personale dei Sistemi Informativi assegna una casella di posta elettronica generalmente strutturata secondo il modello nome.cognome@iov.veneto.it. La casella di posta elettronica così configurata è denominata "e-mail nominativa". Essendo uno strumento di lavoro, è vietato usare tale indirizzo per fini privati. Le informazioni che transitano nella casella di posta elettronica nominativa sono considerati dati aziendali.
L'utente assegnatario è responsabile del corretto utilizzo della propria casella di posta elettronica. In particolare, la casella di posta deve essere mantenuta in ordine, cancellando documenti non più utili ed allegati ingombranti e che non sono necessari ai fini dell'attività lavorativa.
A titolo esemplificativo e non esaustivo l'utente non può utilizzare la posta elettronica per:

- Invio e/o il ricevimento di allegati contenenti filmati o brani musicali (mp3) non legati all'attività lavorativa;

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

- Partecipazione a catene telematiche (o "di Sant'Antonio"). L'utente che ricevesse messaggi di tale tipo, lo dovrà comunicare immediatamente al personale dei Sistemi Informativi, senza aprire gli allegati contenuti in tali mail;
- Inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, orientamento sessuale, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita;
- L'iscrizione o la partecipazione a forum, mailing list, concorsi, partecipazione a dibattiti, corsi, aste online, siti web o social network utilizzati per scopo personale o comunque non attinenti alla mansione assegnata.

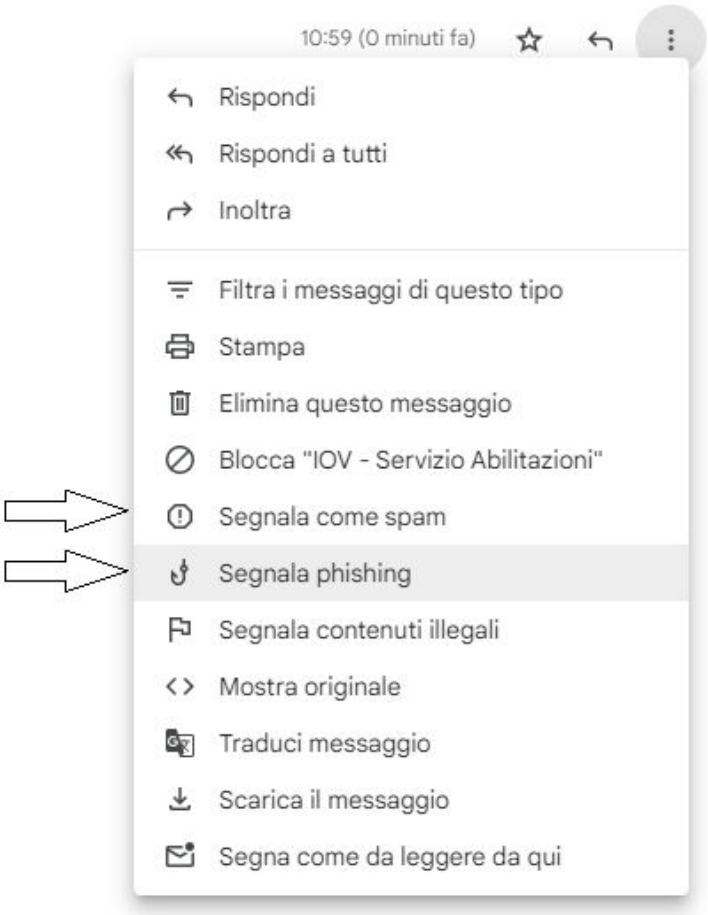
Non è possibile attivare l'invio automatico di e-mail all'indirizzo di posta elettronica privato, ad esempio attivando un "inoltro" automatico della posta in arrivo, nemmeno in caso di assenza prolungata dal servizio, salvo esplicita autorizzazione da parte dei Sistemi Informativi.

L'utilizzo di caselle di posta elettronica personali private (quindi NON in dominio @iov.veneto.it) è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale: in tali casi l'utilizzo di tale canale deve riguardare esclusivamente informazioni di carattere generale, non contenenti alcun dato di natura personale, e senza prevedere l'invio di alcun allegato contenente dati aziendali. Il dipendente è responsabile della corretta gestione della casella di posta personale, qualora utilizzata per queste finalità, ivi comprese le misure di sicurezza applicate sul dispositivo utilizzato.

La posta elettronica è uno strumento di scambio di informazioni, dati e documenti e viene, quindi, utilizzata per la condivisione degli stessi; non è uno spazio idoneo a conservare dati e documenti, i quali vanno archiviati negli spazi dedicati forniti dallo IOV-IRCCS (cartelle di condivisione, gestionale per il protocollo, applicativi software specifici per determinate attività).

Nel caso in cui un utente riceva una e-mail da mittenti sconosciuti, di phishing, spam o sospetta, per non incorrere nel rischio di essere infettati da virus, dovrà riporre tale messaggio nella sezione "phishing". L'utente non dovrà aprire nessun link e nessun allegato presenti nella mail. Come si può vedere dall'immagine di seguito riportata, è possibile segnalare la mail come "phishing" selezionando la relativa voce nel menu a tendina che si apre cliccando sui tre pallini in alto a destra.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*



L'utente dovrà contattare quanto prima l'Help Desk per avvisare di tale rischio. Risulta, quindi, importante porre la massima attenzione nell'apertura di file allegati ai messaggi di posta elettronica prima del loro utilizzo, anche nel caso di messaggi provenienti da mittenti conosciuti, ma che contengano allegati sospetti (ovvero file con estensione .cab, .exe, .scr, .pif, .bat, .cmd, altro). Questa regola vale anche per le e-mail che si ricevono contenenti collegamenti a siti web o ftp per il download di file, che non devono essere aperti, ma devono essere spostati nella sezione "segnala phishing" della casella di posta elettronica aziendale, contattando poi l'Help Desk per mettere al corrente dell'episodio.
Per la trasmissione di file, fatto salvo quanto previsto nei precedenti capitoli, è opportuno utilizzare le cartelle condivise messe a disposizione dall'Istituto oppure lo spazio Drive. È possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non deve mai superare i 15 MB.
Informazioni o dati di categoria particolare (c.d. dati sensibili), di cui all'art. 9 GDPR, possono essere inclusi nelle e-mail solo in relazione alle mansioni affidate e tra destinatari autorizzati al trattamento. In ogni caso non possono essere comunicati a e-mail non istituzionali, se non con canali protetti o con modalità tali da consentirne la massima riservatezza (es. invio allegati compressi protetti da password comunicata separatamente su altri canali).
È fatto divieto di divulgare notizie, dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperti dal segreto professionale cui sono tenuti i dipendenti e collaboratori in ottemperanza agli obblighi di fedeltà e correttezza.
In caso di assenze programmate (ferie, permessi, attività di lavoro fuori sede dell'assegnatario della casella) ovvero prolungate, per motivi di altra natura è buona regola che l'utente imposti un messaggio automatico per esplicitare il periodo di assenza e le modalità di contatto del servizio di appartenenza.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Il personale dei Sistemi Informativi nei casi descritti all'art. 5.19 e al fine di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, su autorizzazione della Direzione dell'Istituto, potrà accedere alla casella di posta elettronica per le sole finalità ivi indicate. L'accesso ai contenuti della corrispondenza nella casella di posta elettronica avviene esclusivamente in caso di assenza prolungata o impedimento dell'utente che lo rendono indispensabile ed indifferibile. L'accesso sarà comunicato preventivamente all'utente o, in caso di impossibilità oggettiva, successivamente. Le operazioni d'accesso saranno sempre oggetto di verbalizzazione.
Le comunicazioni inviate e ricevute tramite la casella di posta aziendale vengono conservate per tutto il periodo di assegnazione della stessa ovvero fino al superamento del limite di spazio consentito per la casella. Al superamento di detto limite è responsabilità dell'assegnatario provvedere a liberare lo spazio necessario.
In caso di cessazione dall'incarico presso lo IOV, i Sistemi Informativi procederanno alla sospensione dell'account conservando il contenuto della cartella di posta elettronica per 3 mesi; successivamente si procederà all'eliminazione dell'account che comporta la cancellazione del contenuto. Casi particolari di richieste o esigenze verranno valutate di volta in volta in collaborazione con l'Ufficio Privacy.
Invece, in caso di assenza temporanea dal servizio per incarichi presso altri Enti, l'account di posta elettronica e il relativo contenuto verrà temporaneamente sospeso con la possibilità di riattivazione al rientro in servizio.
Il traffico generato dal sistema di posta elettronica è soggetto a registrazione mediante appositi "file di log" nei quali sono memorizzati, tra le varie attività associate al proprio account, gli identificativi di mittente e destinatari, l'oggetto del messaggio, la data e ora del messaggio e l'ID-Messaggio.
Il dipendente è responsabile del contenuto dei messaggi inviati e si deve uniformare alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'Azienda nel presente Regolamento. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

Art. 5.14. Accesso in lavoro a distanza (telelavoro e lavoro agile)

L'Ente si fa carico di formare l'utente all'utilizzo della sua postazione remota virtualizzata, fornendogli le istruzioni e le credenziali per l'accesso. La postazione virtualizzata è in tutto e per tutto assimilabile a una postazione fisica, quindi soggetta alle medesime regole e limitazioni generali sopra esplicitate.
In aggiunta a quanto già espresso precedentemente, durante l'utilizzo della postazione virtuale:

- è vietato trasferire tra la postazione virtuale e la postazione personale qualsiasi file o documento di qualsiasi forma o origine, in entrambe le direzioni;
- è rimarcato il divieto assoluto di salvare file aziendali sul proprio dispositivo personale;

L'utente è considerato responsabile per qualsiasi danno causato all'Ente derivante dall'utilizzo improprio della postazione virtuale dal proprio dispositivo personale, sia per imperizia sia per dolo (passaggio di virus/malware, data breach, ecc.).
Qualora il personale abbia in dotazione un portatile aziendale, si raccomanda l'utilizzo dello stesso invece di un dispositivo personale per l'attività di telelavoro o lavoro agile. Per completezza, si rimanda al Regolamento Lavoro Agile condiviso dalle Risorse Umane (Regolamento Lavoro Agile, approvato con DDG n. 928 del 30/10/2023).

Art. 5.15. Uso dei social network

Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione e al libero scambio di idee ed opinioni, l'Istituto ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine e il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partner, oltre agli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dall'Istituto, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti dello stesso Istituto Al fine di assicurare il rispetto del segreto d'ufficio,

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

del segreto professionale e della riservatezza dei dati conosciuti in ambito aziendale, è vietato l'uso dei social network sia aziendali sia privati per lo scambio di informazioni e dati inerenti l'attività istituzionale.
La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Istituto riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui fornitori e altri partner dell'Ente stesso. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi sia dell'Istituto. L'utente, nelle proprie comunicazioni, non potrà, quindi, inserire marchi o altri segni distintivi dell'Istituto, né potrà pubblicare disegni, modelli o altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà, peraltro, avvenire solo previa specifica autorizzazione della Direzione Generale dell'Istituto.
L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori dell'Istituto, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro dell'Istituto, se non con il preventivo consenso del Responsabile d'ufficio.
L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Istituto, i colleghi, i clienti e i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo sono, quindi, vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito di lavoro di IOV-IRCCS.
Infine, in via generale e ove non autorizzato in senso diverso dal proprio Responsabile d'ufficio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Istituto, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Istituto.
È vietato l'utilizzo dell'account di posta elettronica istituzionale "nome.cognome@iov.veneto.it" per l'iscrizione a social network. L'utilizzo di social network a fini istituzionali è consentito solo a determinate Unità Operative come l'Ufficio Comunicazione e Marketing.
Si segnala che i Sistemi Informativi possono effettuare controlli sull'uso improprio degli account di posta elettronica associati a social network o altri servizi online o non autorizzati, come riportato nel DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 giugno 2023, n. 81: *L'amministrazione, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali. In caso di uso di dispositivi elettronici personali, trova applicazione l'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005, n. 82.*

Art. 5.15.1. Utilizzo di chatbot o altri sistemi basati su intelligenza artificiale

Considerata la larga diffusione e facilità di accesso a strumenti di intelligenza artificiale generativa, anche in forma gratuita; considerato che questi strumenti possono essere di aiuto e stimolo nell'attività lavorativa quotidiana, l'utilizzo, senza costi a carico dell'Istituto, è generalmente consentito. Tuttavia, è severamente vietato inserire dati personali, informazioni riservate o segreti aziendali nei prompt o nelle interazioni con chatbot basati su modelli linguistici di grandi dimensioni (LLM), come Claude, ChatGPT o simili. Questa proibizione si applica a qualsiasi informazione confidenziale, inclusi ma non limitati a: dati personali e di natura particolare ai sensi dell'art. 9 e 10 GDPR riferibili a pazienti e personale IOV, ma anche dati finanziari, strategie aziendali, progetti in fase di sviluppo e qualsiasi altra informazione non di dominio pubblico.

Art. 5.16. Dati aziendali

I dati devono essere trattati con liceità e correttezza. Il trattamento dei dati è ammesso solamente per uno scopo determinato, esplicito e legittimo.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

I dati oggetto di trattamento devono essere pertinenti, non eccedenti e completi rispetto alle finalità perseguite; nel caso di trattamento di dati sensibili o giudiziari, devono essere trattati i dati indispensabili per gli scopi del proprio agire. Per motivi di sicurezza non è possibile salvare le informazioni confidenziali all'interno del dispositivo elettronico e/o su supporti rimovibili, ma è necessario salvare tali informazioni sulle cartelle di rete aziendali messe a disposizione.
Nel caso in cui supporti esterni sono consegnati a terzi per trasferire dati, assicurarsi che sugli stessi siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, operando in modo tale da non permettere a terzi di copiare le informazioni aziendali memorizzate.
Eliminare documenti, dischetti o altri supporti di memorizzazione in maniera sicura, evitando di gettarli via senza averli previamente resi inutilizzabili.
Si ricorda che la semplice cancellazione/eliminazione dei dati dai dispositivi di memorizzazione non preclude il futuro recupero, a meno di non effettuare particolari attività formattazione a basso livello in carico ai Sistemi Informativi.
Accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutili messaggi di posta elettronica. La posta elettronica aziendale deve essere utilizzata come servizio di messaggistica, non di archivio.
È severamente vietato conservare copie, anche parziali, dei dati aziendali, su dispositivi personali.

Art. 5.16.1. Esportazione dati

I beni e le risorse informatiche, i servizi IT (Information and Technology) e le reti informatiche costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'Istituto. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ogni utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per lo IOV), e comunque per l'esclusivo perseguimento degli obiettivi aziendali.
A tal fine si precisa che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche dell'Istituto, sarà dallo stesso considerato come avente natura aziendale e non riservata personale. Pertanto è vietata l'esportazione di qualsiasi file trattato attraverso le risorse informatiche dello IOV, a titolo esemplificativo, su supporti mobili (oppure su servizi cloud) salvo esplicita indicazione e autorizzazione. In particolare è vietato lo spostamento di tali file in altri spazi di archiviazione per farne poi un uso personale oppure per attività lavorativa con diverso titolare al trattamento dati, ad eccezione di eventuali accordi contrattuali specifici autorizzati espressamente dalla Direzione.

Art. 5.16.2. Conservazione e archiviazione informatica dei dati

Lo IOV-IRCCS mette a disposizione dei lavoratori spazi di archiviazione per documenti in formato digitale. Tali spazi includono:

- cartelle di rete, rese fruibili tramite dalle postazioni collegate alla rete aziendale
- spazi di archiviazione cloud.

I dati sensibili e le categorie particolari di dati, a chiunque riferiti (i.d. utenti, pazienti, personale IOV, collaboratori esterni, visitatori, etc.) vanno archiviati e conservati negli spazi specificamente previsti e adeguatamente protetti per evitare accessi impropri e/o indesiderati da parte di utenti non autorizzati.

Art. 5.16.3. Archiviazione e trasmissione informatica di dati particolari

I dati particolari costituiscono un elemento fondamentale per le attività di ricovero, di cura e di ricerca perseguite dallo IOV-IRCCS. Considerata la loro delicatezza, i dati particolari sono trattati per finalità esplicite, legittime e determinate, in modo non eccedente il perseguimento delle finalità stesse, nel rispetto del principio di minimizzazione del dato.
Il trattamento dei dati particolari avviene utilizzando in modo sicuro gli strumenti digitali messi a disposizione dei lavoratori. Pertanto non è consentita l'archiviazione dei dati su sistemi non esplicitamente destinati a tale scopo. In particolare, la cartella clinica elettronica e il sistema di gestione dei referti ambulatoriali sono considerati adeguati all'archiviazione dei dati particolari.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

Risulta vietato salvare dati di natura particolare, referti, immagini diagnostiche e tutto ciò che riguarda la storia clinica di un paziente, su cartelle di rete condivise o altri spazi non autorizzati, ovvero tutto ciò che non è la cartella clinica elettronica ed il sistema di gestione dei referti ambulatoriali. La condivisione di dati aziendali e personali o file aziendali riservati è consentita, previa autorizzazione del proprio Responsabile, mediante canali di comunicazione sicura e protetta messi a disposizione dall'istituto. L'eventuale invio di dati mediante e-mail aziendale è consentito solo previa autorizzazione del proprio responsabile e solo se protetti da password, facendo attenzione a inviare la password con un canale di comunicazione diverso dalla e-mail (es. sms, chiamata). Non è consentito inviarla con altri mezzi messi a disposizione dal provider del servizio di posta elettronica aziendale.
Non è consentito l'accesso a enti terzi ai servizi di storaging aziendali salvo espressa autorizzazione da parte dei Sistemi Informativi aziendali previa consultazione e parere dell'Ufficio Privacy.
La persona che condivide i dati con l'esterno si assume la responsabilità di eventuali danni che possono derivare da un uso improprio di queste informazioni, sia per imperizia che per dolo.

Art. 5.17. Gestione degli incidenti e Data Breach

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato in modo tempestivo ai Sistemi Informativi tramite il servizio di Help Desk, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative. Per la categoria di incidenti Data breach tutto il personale in servizio presso lo IOV-IRCCS si attiene alla procedura interna per la gestione degli eventi potenzialmente qualificabili come tali.

Art. 5.18. Osservanza delle disposizioni in materia di privacy

Tutti i soggetti a cui si applica il presente Regolamento devono osservare le disposizioni in materia di protezione dei dati personali ai sensi della normativa vigente e le misure per la sicurezza di dati e sistemi identificate dall'Istituto.

Art. 5.19. Accesso ai dati trattati dall'utente

È facoltà dell'Istituto, tramite il supporto del personale dei Sistemi Informativi, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti.
L'Istituto rende noto che il personale incaricato che opera presso la UOC Sistemi Informativi è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, i Sistemi Informativi ne daranno comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso con apposito verbale.
Potrebbe rendersi necessario anche l'accesso anche ai tabulati del traffico telefonico sia per motivi di sicurezza del sistema informatico che per finalità di controllo e programmazione dei costi aziendali, come la verifica dei costi di connessione ad Internet, traffico telefonico, altro.

Art. 5.20. Sistema di controlli graduali

Per tutelare il patrimonio aziendale e garantire la sicurezza del lavoratore anche in relazione ai pericoli derivanti dall'uso delle tecnologie digitali, lo IOV-IRCCS può svolgere dei controlli sull'utilizzo degli strumenti informatici messi a disposizione del personale dello IOV-IRCCS stesso. Tali controlli saranno svolti dal personale incaricato solo in seguito ad anomalie segnalate e/o riscontrate.
I controlli verranno effettuati in maniera graduale e potranno comportare avvisi generalizzati rivolti alle singole

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*

aree o Unità Operative in cui è stata rilevata l'anomalia.
Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie e per i casi di particolare gravità previa autorizzazione della Direzione.
In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 5.21. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni del presente Regolamento.
La mancata osservanza del Regolamento, ferma l'eventuale responsabilità del dipendente in sede disciplinare, potrà essere valutata anche in sede giudiziale nei casi di maggiore gravità.

Art. 5.22. Norma di rinvio

Per tutto quanto non previsto dal presente Regolamento si rinvia alla normativa statale e regionale di riferimento.

Art. 5.23. Entrata in vigore

Il presente Regolamento entra in vigore nel quindicesimo giorno successivo a quello della pubblicazione della relativa deliberazione di approvazione nell'Albo on-line istituzionale.

Il presente documento è proprietà dell'Istituto Oncologico Veneto IRCCS *e ne è vietata ogni forma di divulgazione non espressamente autorizzata*