

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 1 di 12

Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi elettronici

INDICE

Art. 1	Scopo	2
Art. 2	Campo di applicazione del Regolamento	2
Art. 3	Definizioni	2
Art. 4	Responsabilità	3
Art. 5	Disposizioni	4
Art. 5.1	Utilizzo del Personal Computer e accesso da parte della UOS Sistemi Informativi	4
Art. 5.2	Gestione ed assegnazione delle credenziali di autenticazione	5
Art. 5.3	Utilizzo della rete dell'Azienda ULSS 1 e controlli da parte della UOS Sistemi Informativi	6
Art. 5.4	Utilizzo e conservazione dei supporti rimovibili	6
Art. 5.5	Utilizzo di PC portatili	7
Art. 5.6	Uso della posta elettronica, accesso da parte di altri utenti e controlli da parte del Servizio Sistemi Informativi	7
Art. 5.7	Navigazione in Internet e controlli da parte della UOS Sistemi Informativi	9
Art. 5.8	Protezione Antivirus	10
Art. 5.9	Utilizzo dei telefoni	10
Art. 6	Osservanza delle disposizioni in materia di Privacy	11
Art. 7	Controlli e accesso ai dati trattati dall'utente	11
Art. 8	Sanzioni	11
Art. 9	Aggiornamento, archiviazione, pubblicazione e conservazione	11

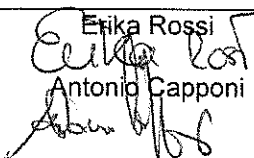
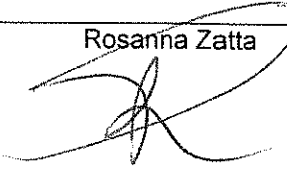
Gruppo di lavoro

Alessandra De Nardi – UOS Sistemi Informativi

Erika Rossi – UOS Internal auditing

Damiano Neso – Consulente UNIS&F

Edizione	Rev.	Data	Descrizione modifiche
1	0	12/05/2018	Delibera n. 1169 del 27/07/2018 1 ^a approvazione del Direttore Generale
2	0	29/08/2019	Delibera n. 1276 del 19/09/2019 2 ^a approvazione del Direttore Generale
3	0	10/06/2021	Delibera n. <u>705</u> del <u>14.06.2021</u> 3 ^a approvazione del Direttore Generale

REDAZIONE	VERIFICA	APPROVAZIONE
Referente gruppo lavoro	Internal Auditing Ufficio Trasparenza e anticorruzione	Direttore Amministrativo
Alessandra De Nardi 	Erika Rossi  Antonio Capponi	Rosanna Zatta 

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 2 di 12

Art. 1 Scopo

Negli ultimi anni l'utilizzo di risorse informatiche (computer, periferiche, software, internet e interconnessioni con altri soggetti) da parte dell'Azienda Ulss 1 Dolomiti (d'ora in avanti Azienda ULSS 1) è notevolmente aumentato sia in termini quantitativi che di complessità degli strumenti messi a disposizione dei propri collaboratori. Tutto ciò ha avuto un'importante implicazione in termini di sicurezza, disponibilità ed integrità dei sistemi informativi dell'ente ed è pertanto necessario stabilire una serie di regole di comportamento che, nel rispetto della normativa in materia di protezione dei dati personali, garantiscano l'efficienza ed il corretto utilizzo delle risorse informatiche ed aziendali.

Si evidenzia, inoltre, che tra i poteri del "datore di lavoro" rientra quello, solitamente riportato nell'ambito del potere direttivo, di controllare l'esatta esecuzione della prestazione lavorativa dovutagli, verificando se il lavoratore usi la prescritta diligenza e osservi le disposizioni impartite, anche al fine dell'eventuale potere disciplinare. Al riguardo si ricorda che, in capo al dipendente pubblico, oltre all'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli a beni mobili ed agli strumenti ad essi affidati, vige l'obbligo di non utilizzare a fini privati materiali o attrezzature di cui dispone per fini istituzionali.

Tuttavia, proprio in considerazione della delicatezza dell'argomento e con riferimento alla normativa in tema di protezione dei dati personali, l'attività di controllo deve essere rispettosa dei principi fondamentali di "proporzionalità" e deve, inoltre, avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato e soprattutto è necessario che di tale attività venga fornita adeguata e preventiva informativa.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda ULSS 1 ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Considerato, inoltre, che l'Azienda ULSS 1, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha, da tempo, deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel Regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

Art. 2 Campo di applicazione del Regolamento

Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, specializzandi, universitari, convenzionati ecc.) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'ULSS 1.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni persona in possesso di specifiche credenziali di autenticazione relative a uno o più applicativi aziendali. Tale figura potrà anche venir indicata quale "persona autorizzata al trattamento".

Art. 3 Definizioni

Titolare del trattamento dati: è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati

R

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 3 di 12

personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nell'Azienda ULSS 1 è il Direttore Generale.

Amministratore di sistema: sono le figure informatiche interne o esterne che accedono con profili più ampi alla gestione o alla manutenzione di un applicativo informatico e rispondono della sicurezza e della salvaguardia del sistema di competenza. Nell'Azienda ULSS 1 gli amministratori di sistema interni sono nominati dal Direttore Generale o dal delegato al trattamento dei dati, per le altre società il Direttore Generale provvede alla nomina dei responsabili esterni del trattamento dei dati con obbligo di notifica dei propri amministratori di sistema al Referente interno Privacy.

Referente interno privacy: è la persona fisica formalmente individuata dal Titolare del trattamento dei dati.

Delegato privacy: sono persone fisiche formalmente individuate dal Titolare del trattamento dei dati. Nell'Azienda ULSS 1 sono i Responsabili delle Unità Operative Complesse (UOC) o Semplici a valenza dipartimentali (UOSD) o Semplici (UOS), i funzionari incaricati con funzioni di coordinamento, gerarchicamente superiori ai singoli utenti che utilizzano gli applicativi e gli strumenti informatici.

Utente: è la persona autorizzata ad accedere alla rete aziendale, ad internet e alla posta elettronica indipendentemente dalla tipologia di rapporto di lavoro che lo lega all'Azienda Ulss 1.

Persona autorizzata al trattamento: è l'utente autorizzato a compiere operazioni di trattamento dati dal titolare o dal responsabile esterno nel rispetto della regolamentazione vigente e delle procedure gestionali adottate dall'Azienda ULSS 1. È individuato dal delegato privacy.

E-mail: indica la funzione di posta elettronica per lo scambio di messaggio e di documenti.

E-mail istituzionale: tutte le caselle non nominative (caselle di reparto/servizio es: direzione.generale@aulss1.veneto.it, medicina.bl@aulss1.veneto.it, informatica@aulss1.veneto.it ecc..)

Download: (in italiano scarico) è l'azione di ricevere o prelevare dalla rete un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente.

Upload: (in italiano, caricamento) 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.

Art. 4 Responsabilità

Oltre a quanto espressamente previsto nel successivo Art. 5, per l'utilizzo degli strumenti di lavoro la responsabilità risiede anche in ordine alle modalità di trattamento dei dati personali gestiti attraverso alcuni degli strumenti stessi, ossia:

- **Il Titolare del trattamento dati:** è responsabile della valutazione dei rischi, della definizione, delle politiche di sicurezza in conformità al Regolamento Europeo 679/2016 e dell'adozione delle misure organizzative adeguate a prevenire e salvaguardare la sicurezza dei dati.
- **Amministratore di sistema:** è responsabile della valutazione, dell'osservazione e dell'adozione di tutte le misure tecniche di sicurezza e trasparenza, delle operazioni di trattamento dei dati dell'applicativo di competenza, in conformità al Regolamento Europeo 679/2016.
- **Referente interno privacy:** a cui competono tutti gli adempimenti in materia di Privacy previsti dal Regolamento Europeo 679/2016, in raccordo con la UOS Sistemi Informativi e con il responsabile della prevenzione e della corruzione per le parti di rispettiva competenza.
- **Delegato privacy:** dovrà provvedere all'organizzazione, alla gestione e alla supervisione di tutte le operazioni di trattamento per conto del titolare che gli sono state formalmente delegate, nonché agire in via strumentale rispetto alle finalità dal medesimo determinate. Dovrà richiedere, per ogni utente di appartenenza, la creazione di un nuovo profilo nel dominio aziendale, la modifica/cancellazione

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 4 di 12

dello stesso ed il rilascio/modifica/cancellazione delle autorizzazioni per l'accesso alle varie procedure aziendali nel rispetto delle procedure gestionali adottate dall'Azienda ULSS 1. Dovrà inoltre vigilare sulla regolare applicazione del presente Regolamento e segnalare al Responsabile della UOS Sistemi Informativi ogni violazione, nonché, qualora si ravvisino gli estremi, attivare le sanzioni previste dall'Art. 8.

- Persona autorizzata al trattamento: deve raccogliere, trattare, archiviare e custodire i dati personali su supporto informatico e/o cartaceo in modo lecito e corretto al fine di ridurre e contenere i rischi di danneggiamento, dispersione, perdita dei dati trattati dall'Azienda ULSS 1, utilizzare gli strumenti di lavoro in modo diligente, corretto e sicuro e nel rispetto della presente regolamentazione di cui dichiara di aver preso visione all'atto di accettazione dell'incarico o della richiesta di rilascio di un nuovo profilo o di una nuova autorizzazione e della regolamentazione vigente in materia di privacy.
- Responsabile della UOS Sistemi Informativi che dovrà regolamentare l'intero processo di utilizzo dei sistemi informatici e di altri dispositivi elettronici nel rispetto della normativa vigente in materia di cyber sicurezza informatica, sicurezza e di privacy ed effettuare i controlli previsti dall'Art. 7 o direttamente o mediante delega formale ad un altro suo collaboratore con rapporto di dipendenza e, qualora si ravvisino gli estremi, attivare le sanzioni previste.

Art. 5 Disposizioni

Art. 5.1 Utilizzo del Personal Computer e accesso da parte della UOS Sistemi Informativi

a) **IL PERSONAL COMPUTER AFFIDATO ALL'UTENTE È UNO STRUMENTO DI LAVORO.** Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento. Inoltre, per i dipendenti pubblici, così come previsto dalla normativa di settore, è vietato un utilizzo a fini privati di materiali o attrezzature di cui dispone per ragioni di ufficio.

b) La postazione di lavoro deve essere utilizzata tenendo presenti, ove possibile, le regole per la razionalizzazione dell'uso delle apparecchiature, quali:

- limitare il numero di copie, incrementando l'utilizzo della posta elettronica per la diffusione e la condivisione dei documenti ed evitare la copia di documenti che possono essere consultati a video;
- adottare la modalità di fronte/retro e preferire la stampa/copia di più pagine per foglio;
- utilizzare, quando possibile, la modalità di copia/stampa in "bozza";
- utilizzare formati ridotti;
- limitare l'uso del colore ove non strettamente necessario;
- assicurarsi che la postazione di lavoro non rimanga accesa al termine dell'orario di lavoro e, se possibile, scollegarla dalla rete elettrica (per esempio spegnendo l'interruttore a muro o la multipresa a cui è collegato).

c) Ogni informazione riservata personale non deve essere memorizzata su cartelle o caselle di posta elettronica aziendale.

d) Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete dell'Azienda ULSS 1 solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto Art. 5.3 del presente Regolamento.

e) Non è consentito il collegamento alla rete aziendale mediante dispositivi non aziendali, salvo specifica richiesta da parte del Delegato privacy e autorizzazione da parte del Responsabile della UOS Sistemi Informativi o suo delegato. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio Sistemi Informativi per conto dell'Azienda ULSS 1, né viene

12

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 5 di 12

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 la stessa Azienda ULSS 1 a gravi responsabilità civili. Si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

f) Salvo preventiva espressa autorizzazione del Responsabile della UOS Sistemi Informativi o suo delegato, non è consentito all'utente di modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

g) Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale della UOS Sistemi Informativi nel caso in cui siano rilevati virus ed adottando quanto previsto dall'Art. 5.8 del presente Regolamento relativo alle procedure di protezione antivirus.

h) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso¹.

i) Sui Personal Computer, di norma, non devono essere memorizzati dati personali e sensibili. Nel caso in cui vengano memorizzati dati personali e sensibili, l'utente risponde della sicurezza e della riservatezza degli stessi e del rispetto dei Regolamenti aziendali.

j) Il personale incaricato dal Responsabile della UOS Sistemi Informativi, anche appartenente ai servizi affidati in outsourcing, ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC e accedere ai dati trattati da ciascuno, su richiesta dell'utente o previa comunicazione formale all'interessato, da effettuarsi anche via email, sulle motivazioni e sulla tempistica dell'intervento, al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus (spyware, malware, etc.) e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). In caso eccezionale di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico e nell'impossibilità di avvisare preventivamente l'utente per non pregiudicare la tempestività ed efficacia dell'intervento, la comunicazione sulla motivazione e sulla necessità dell'intervento potrà essere data anche successivamente.

k) Per garantire la normale operatività dell'Azienda ULSS 1, in caso di assenza prolungata o impedimento dell'utente, l'attività di cui al punto j) potrà essere attivata su richiesta del Delegato Privacy di competenza.

l) Ogni inottemperanza alle disposizioni relative al punto j) e k) dell'Art.5.1 verrà comunicata al Responsabile della UOS Sistemi Informativi.

Art. 5.2 Gestione ed assegnazione delle credenziali di autenticazione

a) Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale della UOS Sistemi Informativi, secondo le procedure gestionali in uso o dagli altri amministratori di sistema

¹ Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente, è quello di adottare il savescreen a tempo con obbligo di reintrodurre la password per l'accesso oppure il blocco del computer.



	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 6 di 12

esterni.

b) 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'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione, senza preventiva autorizzazione da parte della UOS Sistemi Informativi.

c) La parola chiave, formata da lettere (maiuscole e minuscole) e numeri in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato; indicazioni ulteriori potranno essere fornite direttamente all'atto di utilizzo dell'applicativo.

d) È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi.

Art. 5.3 Utilizzo della rete dell'Azienda ULSS 1 e controlli da parte della UOS Sistemi Informativi

a) Per l'accesso alla rete dell'Azienda ULSS 1 ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

b) 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 personali e vanno tenute segrete.

c) Le cartelle utenti presenti nei server dell'Azienda ULSS 1 sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale incaricato dal Responsabile della UOS Sistemi Informativi, anche appartenente ai servizi affidati in outsourcing.

d) Il personale della UOS Sistemi Informativi 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, come già disciplinato all'Art. 5.1.

e) Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Art. 5.4 Utilizzo e conservazione dei supporti rimovibili

a) Tutti i supporti magnetici rimovibili forniti dall'Azienda ULSS 1 (dischetti, CD e DVD riscrivibili, supporti USB, ecc.) contenenti dati particolari (c.d. 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.

b) Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale della UOS Sistemi Informativi e seguire le istruzioni da questo impartite.

c) In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente

2

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 7 di 12

custoditi in armadi chiusi da parte degli utenti.

- d) L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
- e) Se i supporti magnetici contenenti dati sensibili dovessero essere smarriti o rubati, gli utenti devono avvisare tempestivamente l'UOS Sistemi Informativi ed il Referente Interno Privacy per le azioni di competenza.

Art. 5.5 Utilizzo di PC portatili

- a) L'utente è responsabile del PC portatile assegnatogli dalla UOS Sistemi Informativi e deve custodirlo con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
- b) Ai PC portatili si applicano le regole di utilizzo previste dal presente Regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
- c) Sui PC portatili non devono essere memorizzati dati personali e sensibili, né credenziali di accesso alla rete e ai sistemi centrali.
- d) 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.
- e) Tali disposizioni si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, ecc.
- f) I PC portatili vanno restituiti alla UOS Sistemi Informativi al termine del rapporto.
- g) Se i PC portatili dovessero essere smarriti o rubati, gli utenti devono avvisare tempestivamente l'UOS Sistemi Informativi ed il Referente Interno Privacy per le azioni di competenza.

Art. 5.6 Uso della posta elettronica, accesso da parte di altri utenti e controlli da parte del Servizio Sistemi Informativi

- a) **LA CASELLA DI POSTA ELETTRONICA ASSEGNATA ALL'UTENTE E LA CASELLA ISTITUZIONALE SONO STRUMENTI DI LAVORO.** Le persone assegnatarie delle stesse sono responsabili del loro corretto utilizzo anche nel rispetto delle disposizioni in materia di privacy e sicurezza.
- b) Per motivi di sicurezza è fatto divieto di utilizzare le caselle di posta elettronica (@aulss1.veneto.it oppure domini quali @ulss.belluno.it, @ulssfeltre.veneto.it) per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio di default dei messaggi ad altre caselle non aziendali, ravvisando in tal senso un trattamento illecito del dato personale, ovvero non potendo l'Azienda garantire medesimi livelli di sicurezza e protezione sui dati trattati;
 - l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es .mp3) non legati all'attività lavorativa;
 - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;



	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 8 di 12

- la partecipazione a catene telematiche (o di Sant'Antonio). Se l'utente dove, peraltro, ricevere messaggi di tale tipo, deve comunicarlo immediatamente al personale della UOS Sistemi Informativi. Non dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

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

d) È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, tuttavia si ricorda che è stata attivata la casella di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta cartacea.

e) È obbligatorio porre la massima attenzione agli avvisi diffusi dalla UOS Sistemi Informativi e nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non scaricare file eseguibili o documenti di ogni genere da siti Web o Ftp non conosciuti).

f) Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. L'utente può anche reindirizzare i messaggi di posta verso un'altra casella aziendale. Tale funzionalità deve essere attivata dall'utente per garantire l'efficienza delle attività del Servizio.

g) In caso di mancata attivazione della funzionalità di cui al punto precedente o in caso di assenza non programmata o in ogni altra situazione volta a garantire l'espletamento dei procedimenti d'ufficio urgenti e/o rispondere, nei tempi previsti dalla normativa, alle istanze pervenute, sarà comunque consentito al superiore gerarchico o comunque al Delegato Privacy dell'utente, accedere alla casella di posta elettronica nominativa dell'utente, sentendo preventivamente lo stesso, qualora possibile o, in ogni caso, informandolo successivamente.

h) Inoltre, il personale incaricato dal Responsabile della UOS Sistemi Informativi, anche appartenente ai servizi affidati in outsourcing, potrà accedere alla casella di posta elettronica nominativa o istituzionale, previa comunicazione formale all'interessato da effettuarsi anche via e-mail, sulle motivazioni e sulla tempistica dell'intervento, al fine di garantire l'assistenza tecnica e la normale attività operativa del sistema, nonché la massima sicurezza contro virus, spyware, malware, etc. In via eccezionale ed in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico e nell'impossibilità di avvisare preventivamente l'utente per non pregiudicare la tempestività ed efficacia dell'intervento, la comunicazione sulla motivazione e sulla necessità dell'intervento potrà essere data anche successivamente.

i) Ogni inottemperanza alle disposizioni relative al punto h) dell'Art.5.6 verrà comunicata al Responsabile della UOS Sistemi Informativi.

j) Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato simile al seguente:

"La presente comunicazione e gli allegati trasmessi unitamente alla stessa possono contenere informazioni riservate e sono indirizzati esclusivamente ai destinatari qui indicati. L'eventuale risposta alla presente comunicazione inoltre potrebbe essere conosciuta nell'organizzazione di appartenenza del mittente, come indicato nel Regolamento sull'utilizzo del sistema informatico aziendale adottato internamente. Nel caso in cui abbiate ricevuto per errore la presente comunicazione, vogliate cortesemente darcene immediata notizia, rispondendo a

R

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 9 di 12

questo stesso indirizzo di e-mail, e poi procedere alla cancellazione del messaggio dal Vostro sistema. E' strettamente proibito, e potrebbe essere fonte di violazione di legge, qualsiasi uso, comunicazione, copia o diffusione dei contenuti delle comunicazione da parte di chi la abbia ricevuta per errore o in violazione degli scopi della presente (art 616 c.p.; Linee Guida del Garante per posta elettronica ed internet)".

k) Qualora la comunicazione debba essere inviata a più soggetti non appartenenti all'organizzazione aziendale, è necessario provvedere o ad invio singolo, oppure ad invio con declinazione degli indirizzi nel campo "CCN" (copia conoscenza nascosta), così che non vi sia l'indebita condivisione di account con soggetti non autorizzati

l) Informazioni o dati di categoria particolare (c.d. dati sensibili), di cui all'art. 9 GDPR, possono essere inclusi nelle e-mail solo ai fini procedimentali e tra destinatari autorizzati al trattamento. In ogni caso non possono essere comunicati a e-mail non istituzionali, se non con canali protetti.

m) 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.

n) L'utilizzo dei sistemi di posta elettronica è soggetto a norme di comportamento specifiche (c.d. *netiquette*).

5.6.1 Disposizioni particolari per le caselle di posta elettronica "Istituzionali"

La gestione delle caselle istituzionali è autorizzata mediante il meccanismo delle deleghe. La delega consiste nella autorizzazione data al delegato di accedere con le proprie credenziali personali alla casella istituzionale.

La delega viene richiesta dal Delegato Privacy indicando i nominativi che devono essere autorizzati alla gestione della casella istituzionale. L'accesso verrà, pertanto, fatto esclusivamente mediante le credenziali dell'utente nominativo.

Salvo casi espressamente autorizzati, non è consentito l'accesso alla casella istituzionale:

- da computer aziendali (fissi o portatili) esternamente alle sedi dell'azienda;
- da computer non aziendali;
- da dispositivi mobili (cellulari o tablet) sia aziendali che non aziendali.

Il Delegato Privacy è responsabile di mantenere aggiornate le deleghe sulle caselle istituzionali mediante attivazione/disattivazione degli utenti. In particolare, in caso di assenza prolungata o cambio di mansione/servizio/reparto di un dipendente, il Delegato Privacy deve richiedere tempestivamente la disattivazione della delega.

L'UOS Sistemi Informativi, compatibilmente con gli strumenti tecnici messi a disposizione dalla piattaforma di posta elettronica, su richiesta della Direzione Generale, può accedere ai log di registrazione degli accessi effettuati alle caselle istituzionali.

Art. 5.7 Navigazione in Internet e controlli da parte della UOS Sistemi Informativi

a) **IL PC ASSEGNATO AL SINGOLO UTENTE O AL SERVIZIO ED ABILITATO ALLA NAVIGAZIONE IN INTERNET COSTITUISCE UNO STRUMENTO AZIENDALE 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

12

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 10 di 12

lavorativa.

b) In questo senso **l'utente non potrà utilizzare internet**, a titolo puramente esemplificativo in quanto pericolose per la sicurezza del sistema, per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa autorizzazione del Responsabile gerarchicamente superiore e/o dal Responsabile della UOS Sistemi informativi;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, 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 gerarchicamente superiore e/o dal Responsabile della UOS Sistemi informativi.

c) Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, o per ottimizzare utilizzo banda, viene adottato uno specifico sistema di blocco o filtro automatico (white list) che previene determinate operazioni quali l'upload o l'accesso a determinati siti non certificati o inseriti in una black list. Si evidenzia, comunque, che l'utilizzo di sistemi automatizzati preventivi diretti a filtrare l'accesso bloccando determinate categorie di siti potrebbe, a volte, non rivelarsi del tutto idoneo alla piena ed efficace fruizione del sistema informatico e delle modalità di navigazione, rallentandone in modo rilevante la funzionalità: in questa ipotesi, pertanto, si renderebbero necessari controlli successivi all'attività di navigazione diretti a tutelare l'Azienda ed i suoi responsabili da responsabilità, anche penali, connesse a reati commessi con modalità informatiche e telematiche.

d) I controlli, compiuti dal personale incaricato dal Responsabile della UOS Sistemi Informativi, anche appartenente ai servizi affidati in outsourcing, ai sensi del precedente punto, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo e la conservazione dei file stessi non è garantita oltre 6 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda ULSS 1.

Art. 5.8 Protezione Antivirus

a) Il sistema informatico dell'Azienda ULSS 1 è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

b) 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 della UOS Sistemi Informativi.

c) Ogni dispositivo magnetico di provenienza esterna all'Azienda ULSS 1 dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale della UOS Sistemi Informativi.

Art. 5.9 Utilizzo dei telefoni

a) **IL TELEFONO AZIENDALE AFFIDATO ALL'UTENTE È UNO STRUMENTO DI LAVORO.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo, quindi, consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

12

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 11 di 12

b) Qualora venisse assegnato un cellulare aziendale (la concessione dell'utilizzo del cellulare viene rilasciata dalla Direzione Generale) l'utente sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza dell'apposito contratto di servizio a uso privato e in conformità delle istruzioni al riguardo impartite, digitando il prefisso per l'addebito delle chiamate personali al conto privato. Detto uso vale sia per il telefono che per l'utilizzo della banda internet.

c) Se smarriti o rubati, avvisare tempestivamente l'UOS Sistemi Informativi ed il Referente interno Privacy per le azioni di competenza.

Art. 6 Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy, in ottemperanza alle disposizioni del Regolamento UE 679/2016, e alle misure minime di sicurezza per la protezione dei dati personali nello svolgimento delle operazioni di trattamento dei dati secondo le indicazioni scritte e/o verbali fornite dall'Azienda.

Art. 7 Controlli e accesso ai dati trattati dall'utente

a) Si richiamano i controlli di cui ai paragrafi Art. 5.1, Art. 5.3, Art. 5.6, Art. 5.7, Art. 5.9. I controlli sono, per quanto possibile, anonimi o a campione e si concluderanno, qualora si ravvisi un utilizzo irregolare degli strumenti aziendali, con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, con i quali si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

b) Oltre a quanto sopra previsto, e comunque senza alcuna finalità di controllo dell'attività lavorativa, su richiesta documentata della Direzione Generale, il personale della UOS Sistemi Informativi o altro soggetto delegato dalla stessa, può accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti di lavoro informatici aziendali e ai documenti ivi contenuti.

c) In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

d) Nel caso in cui si ravvisino estremi per avviare provvedimenti disciplinari e risarcitori il Responsabile dell'UO interessata dovrà effettuare l'opportuna segnalazione di cui all'art. 8.

Art. 8 Sanzioni

a) 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 con provvedimenti disciplinari e risarcitori previsti dalla normativa vigente, nonché con tutte le azioni civili e penali consentite, attivabili dal Responsabile della UOS Sistemi Informativi o dal Responsabile dell'UO interessata.

Art. 9 Aggiornamento, archiviazione, pubblicazione e conservazione

DOCUMENTO	AGGIORNATO/ ARCHIVIATO da	CONSERV.	LUOGO
REGOLAMENTO	UOS Sistemi Informativi	5 anni	UOS Sistemi Informativi

R

	Regolamento	REG. 12
	Azienda ULSS n.1 Dolomiti	Edizione: 3 Rev. 0 del 10/06/2021
	Regolamento per l'utilizzo dei sistemi informatici e altri dispositivi	Pag. 12 di 12

a) Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte dovranno essere formalmente inviate all'UOS Sistemi Informativi.

b) Il presente Regolamento entra in vigore il giorno successivo alla sua approvazione e può essere oggetto ad aggiornamenti qualora se ne ravvisi la necessità per effetto di intervenute modifiche legislative o di mutamento degli indirizzi interpretativi, fermo restando che le sue disposizioni dovranno intendersi automaticamente sostituite, disapplicate o abrogate nel caso in cui il loro contenuto sia incompatibile con sopravvenute disposizioni di legge.

DIFFUSIONE/PUBBLICAZIONE

Il presente documento è stato oggetto di informativa sindacale, diffuso mediante pubblicazione nell'angolo del dipendente e nell'intranet aziendale.