

**REGOLAMENTO PER L'UTILIZZO DEGLI
STRUMENTI DELL'ENTE**

approvato dalla Deliberazione n. 23/2021

Revisione 01 del

30/09/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

INDICE

1.	SCOPO	2
2.	AMBITO DI APPLICAZIONE	4
3.	RIFERIMENTI	5
4.	DEFINIZIONI	5
5.	DISPOSIZIONI IN MERITO AGLI OBBLIGHI DEI DESTINATARI CON RIGUARDO ALLE MODALITÀ D'USO DEGLI STRUMENTI DELL'ENTE	7
5.1	NORME DI COMPORTAMENTO	7
5.1.1	COMPORTAMENTO PROFESSIONALE	7
5.1.2	CUSTODIA, UTILIZZO E RESTITUZIONE DEGLI STRUMENTI DELL'ENTE	8
5.1.3	MEMORIZZAZIONE E PROTEZIONE DEI DATI	9
5.1.4	GESTIONE DELLE CREDENZIALI DI ACCESSO	9
5.1.5	GESTIONE DEL PROFILO DI ACCESSO	11
5.1.6	SOTTRAZIONE ALLA VISTA DELLE INFORMAZIONI SU SCHERMO	11
5.1.7	UTILIZZO DEI SISTEMI DI RIPRODUZIONE	11
5.2	UTILIZZO DEGLI STRUMENTI DELL'ENTE E POSTAZIONI DI LAVORO	12
5.2.1	STRUMENTI DI REGISTRAZIONE DEGLI ACCESSI	12
5.2.2	POSTAZIONE DI LAVORO	12
5.2.3	INTERNET	12
5.2.4	INTRANET	13
5.2.5	POSTA ELETTRONICA AZIENDALE	13
5.2.6	USO PERSONALE	16
5.2.7	SOFTWARE	16
5.2.8	ANTIVIRUS	17
5.2.9	LIMITAZIONI AL SISTEMA DI CRITTOGRAFIA	17
5.2.10	TELEFONI / TABLET	17
5.2.11	CONTROLLI DA PARTE DI ISTITUZIONE	18
5.2.12	CONSERVAZIONE	20
5.2.13	ALTRI STRUMENTI DELL'ENTE	20
5.2.14	ISTRUZIONI IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO O DI COLLABORAZIONE	20
5.2.15	VIOLAZIONI E SANZIONI	21
5.2.16	OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI	21
5.2.17	ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ	21
5.3	LAVORO DA REMOTO (SMART WORKING, TELELAVORO)	21
6.	ALLEGATI	

Revisione 01 del

30/09/2024



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

SCOPO

Istituzione Veneziana Servizi Sociali alla Persona (di seguito la "**Istituzione**"), per esclusive finalità lavorative/professionali nonché di ricerca, studio e documentazione, può mettere a disposizione mezzi informativo/telematici e l'accesso a Internet quali strumenti di ricerca, archiviazione e lavoro, nonché una casella di posta elettronica aziendale, quale strumento di comunicazione e di condivisione di informazioni strettamente lavorative.

L'Istituzione ha deciso, quindi, di adottare il presente Regolamento per l'utilizzo degli strumenti dell'Ente (di seguito "**Regolamento**") al fine di fornire un quadro preciso di indicazioni ai Lavoratori, e a tutti gli altri Destinatari (definiti *infra, sub §0*), in merito alla modalità di funzionamento degli Strumenti dell'Ente (definiti *infra, sub §0*) loro assegnati o da essi comunque utilizzati, e dunque codificare il set di regole di comportamento da rispettare per un corretto utilizzo dei predetti Strumenti dell'Ente, onde evitare problemi, disservizi e maggiori costi (di manutenzione o di altro tipo) ovvero rischi e/o minacce alla sicurezza dei sistemi e/o dei dati in essi contenuti, con particolare riguardo ai dati personali e/o al patrimonio immateriale della Istituzione, anche ove non tutelato e/o tutelabile attraverso privative.

L'utilizzo degli Strumenti dell'Ente deve sempre ispirarsi ai principi di massima diligenza, buona fede e correttezza; principi, questi, che devono costantemente uniformare e caratterizzare la condotta generale ed i singoli comportamenti di tutti i soggetti autorizzati all'uso dei predetti Strumenti.

Il Regolamento, pertanto, è finalizzato anche ad evitare che i Destinatari possano esporre sé stessi e/o l'Istituzione a sanzioni pecuniarie o penali, derivanti da un uso scorretto o illecito degli Strumenti dell'Ente, nonché esporre Istituzione a serie conseguenze pregiudizievoli, in relazione al suo patrimonio e/o alla sua immagine.

Ulteriore scopo del Regolamento è diffondere una cultura della sicurezza che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.

Scopo del Regolamento è anche quello di recepire e dare attuazione alle disposizioni normative e ai principi previsti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito "**GDPR**"), nonché dei Provvedimenti emanati dal Garante per la protezione dei dati personali (di seguito "**Garante**") al fine di garantire la protezione dei dati personali trattati mediante tali strumenti, nonché la salvaguardia del patrimonio informativo aziendale, gli standard qualitativi dei servizi resi ed il know-how di Istituzione (costituito da dati, notizie ed informazioni di carattere strettamente riservato e confidenziale) da parte di coloro che agiscono nella struttura della Istituzione o che prestano la propria attività in favore della stessa anche al di fuori della sua struttura, in qualità di lavoratori, indipendentemente dalla natura contrattuale del rapporto professionale in corso.

Al contrario, non rientra tra gli scopi del presente Regolamento il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei suoi dipendenti, che rimangono strettamente vietati e non consentiti.

Pertanto, nel rispetto delle previsioni di cui agli artt. 4 e 8 della Legge 20 maggio 1970, n. 300 (di seguito "**Statuto dei Lavoratori**"), Istituzione intende anche disciplinare, con il Regolamento, le modalità di raccolta ed utilizzo delle informazioni e dei dati trattati tramite gli Strumenti dell'Ente, informando circa l'esercizio dell'eventuale potere disciplinare nei confronti del Personale, qualora si verificasse ed accertasse - secondo le procedure e nel rispetto delle garanzie e tutele oggetto delle previsioni che seguono - un uso improprio e/o non autorizzato degli Strumenti dell'Ente assegnati e/o in loro dotazione.

Revisione 01 del

30/09/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Il Regolamento e le previsioni ed indicazioni in esse contenute integrano dunque:

- a) l'apposita informativa resa da Istituzione, ai sensi e per gli effetti dell'art. 4 dello Statuto dei Lavoratori, quanto al Personale, e in ogni caso dell'art. 13 del GDPR, in ordine alle modalità, finalità, procedure e relative tutele con riferimento al trattamento dei loro dati personali nel caso in cui si procedesse ad eventuali attività di controllo effettuate dalla stessa, anche attraverso strumenti di registrazione degli accessi e delle presenze (ad esempio *badge*, rilevatori magnetici o elettronici) o mediante verifiche sull'utilizzo degli Strumenti dell'Ente in loro dotazione per motivi professionali (ad esempio PC, *tablet*, *smartphone* dell'Ente), nonché della rete internet e della posta elettronica aziendale. L'informativa sulla privacy può essere consultata all'interno della cartella condivisa denominata "Istituzione Veneziana".
- b) le specifiche istruzioni già fornite al personale dell'Istituzione nella lettera di designazione dei "Soggetti Autorizzati al Trattamento".

AMBITO DI APPLICAZIONE

Il Regolamento si riferisce ai trattamenti di Dati Personali (definiti *infra*, sub §0) effettuati da Istituzione attraverso gli Strumenti dell'Ente, per le finalità di seguito indicate:

- esecuzione della prestazione lavorativa da parte dei Lavoratori;
- gestione della sicurezza del traffico elettronico e telematico;
- accesso agli Strumenti dell'Ente in caso di assenza del Lavoratore;
- *incident management* e *troubleshooting*;
- eventuali procedure amministrative e procedimenti disciplinari, a seguito dei controlli posti in essere con le finalità e secondo le modalità specificate nel successivo paragrafo 0;

Il Regolamento si applica a tutti i soggetti che utilizzano gli Strumenti dell'Ente, a prescindere dalle relative finalità, tra cui, a mero titolo esemplificativo e non esaustivo:

- a) lavoratori subordinati, anche con contratto a termine, in ogni caso senza distinzione di durata, orario, ruolo, funzione e/o livello (ivi inclusi i dirigenti) e/o modalità di svolgimento della prestazione, compresi anche i lavoratori in cd. "telelavoro" o in cd. "smart working" (di seguito anche solo il "Personale");
- b) lavoratori autonomi, a prescindere dal rapporto contrattuale intrattenuto;

Tutti i soggetti sopra elencati saranno di seguito, congiuntamente, indicati come "Lavoratori".

Il Regolamento costituisce anche espressione dei doveri di correttezza comportamentale e diligenza contrattuale e costituisce parte integrante del complessivo sistema normativo aziendale. In ogni caso, il Oltre ai Lavoratori, il presente Regolamento si applica altresì a qualunque soggetto che si trovi in possesso di specifiche credenziali di autenticazione per l'accesso alla rete informatica utilizzata da Istituzione o che comunque utilizzi, a qualsiasi titolo, anche in via temporanea, gli Strumenti dell'Ente, in qualunque sede e/o ufficio, anche riconducibile alla struttura di quest'ultima, al fine di proteggere e mantenere riservati i dati trattati e di evitare che, attraverso l'eventuale utilizzo di tali strumenti possa essere esposta a rischi di natura patrimoniale e a responsabilità conseguenti alla violazione di specifiche norme di legge.

I soggetti di cui sopra, unitamente ai Lavoratori, saranno di seguito congiuntamente indicati come "Destinatari".

Il Regolamento si applica sia nel caso che Istituzione ricopra la funzione di Titolare del trattamento, che di Responsabile del trattamento. Per le definizioni di "Titolare del trattamento" e di "Responsabile del trattamento" si rimanda al paragrafo 0, "Definizioni".

Revisione 01 del 30/06/2024

Dorsoduro 943 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5293049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

RIFERIMENTI

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("GDPR");
- Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016" (di seguito anche solo il "Decreto");
- Opinion 2/2017 del cd. "Article 29 Data Protection Working Party" dell'8 giugno 2017, "on data processing at work";
- Provvedimento del Garante del 1° marzo 2007, "Lavoro: le linee guida del Garante per posta elettronica e Internet", pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007 (di seguito anche solo il "Provvedimento");
- Provvedimento del Garante del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato in Gazzetta Ufficiale n. 300 del 24 dicembre 2008 (di seguito anche solo il "Provvedimento AdS");
- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento" ("Statuto dei Lavoratori");
- Legge 22 aprile 1941 n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (di seguito anche solo "Legge sul Diritto d'Autore");
- Decreto Legislativo 10 febbraio 2005, n. 30 (di seguito anche solo "Codice della proprietà industriale");
- le previsioni di cui al CCNL "2016 - 2018" del Comparto Funzioni Locali, applicato da Istituzione (di seguito anche solo "CCNL").

DEFINIZIONI

Ferme le definizioni già previste nei paragrafi precedenti, le parole e le espressioni di seguito indicate hanno il seguente significato:

- **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile: si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Interessati:** persone fisiche, identificate o identificabili, alle quali si riferiscono i Dati Personali.
- **Trattamento:** qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.
- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno ad Istituzione, che tratta dati personali per conto della stessa, ai sensi dell'art. 28 GDPR.

Revisione 01 del

20/09/2024

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

- **Data Breach:** la violazione 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.
- **Normativa Applicabile:** il GDPR e le disposizioni di cui al Decreto, gli artt. 4 e 8 dello Statuto dei Lavoratori, il CCNL, la Legge sul Diritto d'Autore, il Codice della Proprietà Industriale nonché il Provvedimento e tutti gli ulteriori provvedimenti e linee guida del Garante comunque applicabili.
- **Strumenti dell'Ente:** Tutte le dotazioni hardware e software e le risorse informatiche e/o telematiche dell'Ente della Istituzione.
- **Antivirus:** un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi;
- **Back Up:** operazione tesa a creare una copia di sicurezza delle informazioni (dati o programmi).
- **Chat line:** servizio che mette in contatto due o più utenti per una comunicazione in tempo reale;
- **Compact Disc:** supporto di memorizzazione di informazioni in formato digitale;
- **DVD:** supporto di memorizzazione ottico delle informazioni;
- **File di Log:** file nel quale vengono registrate cronologicamente tutte le informazioni relative alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, base dati); particolari file di log sono quelli relativi ai log di Amministratore di Sistema che registrano tutte le attività di accesso ai sistemi eseguite dagli Amministratori di Sistema;
- **File Server:** area di archiviazione informatica presente sul server aziendale;
- **Freeware:** software che viene distribuito in modo gratuito;
- **Gestore dell'applicazione:** soggetto nominato responsabile di autorizzare gli accessi degli utenti alle applicazioni di cui è gestore;
- **Hardware:** qualunque arte fisica di un personal computer;
- **Hard Disk:** dispositivo di memoria di massa che utilizza uno o più dischi magnetici per l'archiviazione dei dati;
- **Laptop/PC:** personal computer portatile;
- **Log in:** attività volta ad identificare una utenza per l'accesso ad un computer o ad una applicazione informatica tramite inserimento di User ID e Password;
- **Mailing list:** un sistema organizzato per la condivisione via mail di un argomento a più persone;
- **Network:** insieme di sistemi per l'elaborazione delle informazioni messi in comunicazione fra loro;
- **Password:** parola segreta associata ad un User ID;
- **Password di boot:** password necessaria per l'accensione del personal computer e il seguente avvio dei programmi in esso installati;
- **Password recovery:** attività di recupero di una password dimenticata o smarrita;
- **Phishing:** attacco ingannevole, su Internet, per indurre un utente a rivelare informazioni personali e/o dell'Ente (quali credenziali di accesso, codici, ecc.);
- **Peer-to-Peer:** tipologia di rete informatica caratterizzata da ridotti livelli di protezione;
- **Repository documentali:** risorse informatiche (dischi, aree di memoria ecc.) dove sono conservate le immagini fisiche dei documenti acquisiti con sistemi di scansione, organizzati per classe assieme ai riferimenti necessari (indici o tag) per la loro identificazione e ricerca;
- **Sandbox:** spazio separato, all'interno di un *device mobile*, per l'esecuzione sicura di programmi e/o applicazioni e/o per la memorizzazione sicura di dati;
- **Screen Saver:** applicazione per computer che provoca lo standby del PC dopo un periodo programmato di inattività del mouse e della tastiera, impostabile attraverso un timer;
- **Serial code:** codice di identificazione di autenticità di un software che l'utente deve inserire per dimostrare l'autenticità della propria copia;

Revisione 01 del

30/09/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5280182 - Fax - 041 5280049 - C.F. 00012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

- **Server:** componente informatica che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete;
- **Smart Card:** dispositivo hardware delle dimensioni di una carta di credito che possiede potenzialità di elaborazione e memorizzazione dati ad alta sicurezza;
- **Software:** programma o un insieme di programmi in grado di funzionare su un elaboratore;
- **Spoofing:** attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità;
- **User ID:** codice identificativo associato ad una persona o ad un gruppo;
- **Virus:** un software che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, potendo provocare danni sia al software che all'hardware;
- **Wireless:** sistema di comunicazione tra dispositivi elettronici, che non fanno uso di cavi.

DISPOSIZIONI IN MERITO AGLI OBBLIGHI DEI DESTINATARI CON RIGUARDO ALLE MODALITÀ D'USO DEGLI STRUMENTI DELL'ENTE

Norme di Comportamento. Comportamento professionale

Istituzione stabilisce le misure tecniche ed organizzative per assicurare la riservatezza e l'integrità delle informazioni e dei dati trattati con gli Strumenti dell'Ente, in accordo con la Normativa Applicabile. È fatto assoluto divieto di cedere a terzi gli Strumenti dell'Ente, anche in parte (ad esempio, SIM o auricolari), o comunque di consentirne l'utilizzo da parte di terzi non autorizzati da Istituzione.

Tutti gli Strumenti dell'Ente devono essere correttamente custoditi e mantenuti in buono stato dai Destinatari che devono contribuire, in rapporto ai propri ruoli, competenze e responsabilità, alla protezione dell'intero patrimonio. È responsabilità dei Destinatari richiedere gli interventi manutentivi opportuni, segnalando tale necessità alla società Venis S.p.A. già nominata responsabile del trattamento (di seguito denominata "Amministratore di Sistema") attraverso il gestionale messo a disposizione da quest'ultima denominato "Ticket".

Costituisce regola generale che l'utilizzo degli Strumenti dell'Ente deve essere limitato e strettamente vincolato all'esercizio di attività lavorative/professionali, di ricerca e documentale. Salve eventuali deroghe in particolare, è vietato:

- utilizzare gli Strumenti dell'Ente per uso personale;
- impiegare gli Strumenti dell'Ente per finalità diverse da quelle per i quali sono stati progettati o utilizzare i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all'organizzazione;
- recare volontariamente danni ai sistemi informativi, agli strumenti di supporto, ed in generale agli Strumenti dell'Ente utilizzati da Istituzione.

"Pasta che gli Strumenti dell'Ente possono essere utilizzati esclusivamente per svolgere le attività lavorative/professionali meglio descritte nei paragrafi precedenti, può tuttavia consentire l'uso di Internet per ragioni personali, in via occasionale ed eccezionale, esclusivamente per risolvere eventuali urgenze. In ogni caso, non è in alcun modo consentito l'uso personale della posta elettronica aziendale e i Destinatari dovranno, perciò, avvalersi di un indirizzo di posta elettronica personale per tale finalità".

I Destinatari sono tenuti a segnalare immediatamente all'Amministratore di Sistema ogni attività sospetta, rischiosa e/o potenzialmente dannosa e/o, comunque, non conforme al presente Regolamento.

Revisione 01 del

30/09/2024

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Custodia, utilizzo e restituzione degli Strumenti dell'Ente

Memorizzazione e protezione dei dati

L'integrità e la disponibilità delle informazioni e dei dati dell'Ente, ivi inclusi i Dati Personali di titolarità di Istituzione, è garantita solo quando gli stessi sono memorizzati e trattati nell'ambito di sistemi all'uopo specificamente dedicati (ad esempio, *file server*), messi a disposizione da Istituzione ai vari Destinatari.

I Destinatari sono tenuti a trasferire nella pertinente cartella di rete tutti i dati eventualmente presenti nelle memorie fisse o rimovibili dell'Ente del personal computer affidato o comunque messo a loro disposizione, con particolare riferimento ai dati considerati critici o di particolare rilevanza per Istituzione in ragione della loro specifica natura (dati confidenziali, segreti professionali/industriali) ovvero ai dati personali del cui trattamento la Istituzione è titolare o responsabile ai sensi, rispettivamente, degli artt. 24 o 28 GDPR.

Le informazioni archiviate mediante gli – e/o sugli – Strumenti dell'Ente devono essere esclusivamente quelle necessarie all'attività lavorativa. Costituisce buona regola la pulizia periodica degli archivi, da eseguirsi almeno ogni 6 (sei) mesi, con cancellazione dei file obsoleti o inutili.

I supporti di memoria rimovibili dell'Ente (compact disk, hard disk USB, pen flash USB, ecc.) devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave). È sempre necessario verificare il contenuto informativo dei supporti di memoria, prima della loro consegna a terzi e prima della loro eliminazione/distruzione o sostituzione. In ogni caso, è necessario procedere alla cancellazione dei dati in essi contenuti quando non più necessari.

Se per errore (ad esempio e-mail inviata ad un destinatario errato), o a causa di un malfunzionamento del sistema, i Destinatari dovessero entrare in possesso di informazioni confidenziali, o riservate, o che comunque non sono autorizzati a trattare, saranno immediatamente tenuti a chiudere il programma di visualizzazione e a segnalare l'accaduto e chiedere istruzioni all'indirizzo e-mail eva.clemen@istituzioneveneziana.it del personale interno a ciò adibito affinché siano prese le misure più opportune.

Gestione delle credenziali di accesso

L'accesso a tutti gli Strumenti dell'Ente è sottoposto a procedure di identificazione personale (log-in) di tipo manuale, attraverso la digitazione di un identificativo univoco (User ID) e di una parola segreta (Password) necessari al riconoscimento della identità dei Destinatari da parte del sistema installato sugli Strumenti dell'Ente e/o dell'applicazione in uso.

I Destinatari devono provvedere, sia sui personal computer fissi che portatili, ad impostare la cosiddetta "password di accensione" ovvero di Password di Boot, secondo le modalità indicate, per ognuno degli Strumenti dell'Ente. Al fine di consentire di accedere agli Strumenti dell'Ente in assenza dei Destinatari per ragioni di continuità operativa, i Destinatari stessi sono invitati a comunicare la Password di Boot – con modalità tali da assicurarne la segretezza e prevenirne la comunicazione a terzi e/o la diffusione – ad un fiduciario, l'identità del quale dovrà essere comunicata al personale interno a ciò adibito.

I Destinatari sono tenuti a conservare con la massima cura e segretezza tutte le Password di Boot e/o di accesso alla rete, anche intranet, ed ai sistemi: tali Password devono essere note solo ad essi e non possono essere condivise con altri soggetti, salvo il fiduciario di cui sopra. È comunque vietato ai Destinatari utilizzare

Revisione 01 del

30/09/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5288182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

credenziali di accesso diverse da quelle ricevute (e successivamente aggiornate), in quanto strettamente personali ed assegnate in virtù del ruolo ricoperto, nonché alla luce del rapporto intercorrente con Istituzione.

I Destinatari sono inoltre tenuti a scollegarsi (*log-off*) al termine della sessione di lavoro e/o in caso di assenze dall'ufficio per un lungo periodo di tempo.

In certi casi, Istituzione può predisporre misure di accesso ai sistemi di tipo hardware, mediante l'utilizzo di dispositivi che abilitano direttamente l'accesso o consentono un'ulteriore procedura di identificazione a mezzo password.

In ogni caso, i Destinatari devono seguire alcuni accorgimenti di estrema importanza nella scelta e nella gestione delle proprie credenziali di accesso. In particolare, devono essere esplicitamente rispettate le seguenti regole:

- le Password non devono contenere dettagli personali, anche se in forma parziale, come il proprio nome, la data di nascita, il numero di matricola e/o qualsiasi altro riferimento riconducibile ai Destinatari o alla loro storia personale;
- è vietato ripetere la medesima Password con la sola variazione del carattere numerico (ad esempio password1, password2, ecc.);
- la lunghezza minima delle Password deve essere di almeno 8 caratteri alfanumerici e deve contenere almeno uno tra i primi 3 dei seguenti 4 tipi di caratteri:
 - 1) Lettere maiuscole (A-Z);
 - 2) Lettere minuscole (a-z);
 - 3) Numeri (0-9);
 - 4) Caratteri speciali (es. \$, *, -, ?, ecc);

L'uso dei caratteri speciali, anche se non obbligatorio, è comunque preferibile in quanto aumenta la complessità della Password e di conseguenza la sua sicurezza;

- ogni Password deve avere una validità massima di 90 gg. Trascorso tale termine l'utente è chiamato a cambiarla e, in caso di mancata variazione, il sistema provvederà automaticamente ad interdire l'accesso. L'utente deve provvedere alla sostituzione della Password nel caso in cui essa venga rivelata o si sospetta che questo sia accaduto;
- non è possibile inserire le ultime 10 Password precedentemente utilizzate;
- I Destinatari che accedono a funzionalità applicative dell'Ente che richiedano ulteriori credenziali d'accesso (nome utente/password e/o certificato digitale), oltre a quelle comuni (ad esempio per l'accesso ai personal computer o alla rete aziendale), devono astenersi dall'utilizzare la medesima Password usata per l'accesso ai dispositivi comuni;
- I Destinatari sono responsabili di tutte le attività svolte attraverso l'uso del proprio identificativo personale (User ID); pertanto, non devono rivelare le proprie Password a nessuno, salvo il fiduciario di cui sopra, e devono custodirle in modo appropriato. Allo scopo, le Password non devono mai essere trascritte su fogli, biglietti, post-it o su oggetti, soprattutto se posti nelle vicinanze del PC. Le Password inoltre non devono essere inserite in messaggi di posta elettronica e/o trasmesse attraverso qualsiasi altra forma di comunicazione elettronica, né possono essere salvate su strumenti e/o documenti informatici (ad es. file Word o Excel) che non siano protetti a loro volta da apposite credenziali;
- al fine di consentire la conservazione delle Password, ovvero di accedere agli Strumenti dell'Ente in assenza dei Destinatari per ragioni di continuità operativa, i Destinatari stessi sono invitati a comunicare le stesse, con i relativi User ID – con modalità tali da assicurarne la segretezza e prevenirne la comunicazione a terzi e/o la diffusione – ad un fiduciario.

Revisione 01 del

30/04/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Se lo User ID non viene utilizzato per più di sei mesi viene sospeso. Le credenziali di autenticazione sono disattivate se non usate da almeno 6 (sei) mesi e nel caso in cui il Dipendente dovesse perdere la qualità che gli consente l'accesso ai Dati Personali, così come indicato nella lettera di designazione dei "Soggetti Autorizzati al Trattamento".

Gestione del profilo di accesso

I Destinatari, per ottenere l'abilitazione all'accesso ad un determinato applicativo non incluso nei servizi di base messi a disposizione da Istituzione, devono inoltrare la richiesta di approvazione per l'abilitazione di una nuova utenza (ovvero di modifica di un profilo di accesso), all'Amministratore di Sistema.

Quest'ultimo, per autorizzare la richiesta verifica che il profilo di accesso rispetti il principio di segregazione dei compiti e la coerenza con il ruolo e le mansioni ricoperte dall'utente.

Periodicamente (almeno una volta all'anno) viene effettuata una verifica delle utenze esistenti e dei rispettivi profili di accesso al fine di ridurre il rischio di accessi non autorizzati ai sistemi.

Sottrazione alla vista delle informazioni su schermo

Gli Strumenti dell'Ente e, in particolare, i personal computer non devono essere mai lasciati incustoditi. Anche in caso di breve assenza, il computer deve essere bloccato tramite le funzionalità offerte dal sistema operativo (es. attraverso l'impostazione della modalità "blocca computer" tramite pressione contemporanea dei tasti Ctrl+Alt+Canc).

È opportuno, inoltre, ogniqualvolta ci si allontani dalla postazione di lavoro, disconnettere gli applicativi in uso, selezionando la modalità standby o spegnendo il dispositivo: a tal riguardo, in caso di inattività temporanea dei Destinatari per un periodo superiore ai 15 minuti, si attiverà automaticamente la funzionalità di "salva schermo" (screen saver), al fine di non consentire a terzi di visualizzare lo schermo del dispositivo lasciato incustodito e/o di accedere ai sistemi dello stesso: la funzionalità screen saver è disattivabile mediante digitazione della password per lo "sblocca computer"; tale password è la medesima utilizzata per l'accesso alle risorse di rete.

Al termine della giornata lavorativa, i Destinatari sono tenuti a spegnere tutti gli Strumenti dell'Ente utilizzati o, comunque, loro affidati.

Utilizzo dei sistemi di riproduzione

Gli Strumenti dell'Ente devono essere utilizzati esclusivamente per motivi connessi all'esecuzione della prestazione lavorativa / professionale, anche nel rispetto dei principi di economia.

La produzione di stampe o di copie di documenti, specialmente riservati, deve essere il più possibile contenuta e limitata ai casi di effettiva necessità.

Nell'inviare via fax un documento riservato, i Destinatari non devono utilizzare la funzione di memorizzazione del documento, ma l'invio diretto del documento.

Revisione 01 del

30/09/2024

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 00012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Durante la stampa, fotocopia, scansione o trasmissione via fax di documenti, i Destinatari devono presidiare l'intero processo, al fine di impedire la volontaria o accidentale diffusione di Dati Personali o la perdita di riservatezza sulle informazioni contenute nei documenti stessi. Allo stesso scopo, è dovere dei Destinatari prelevare immediatamente i fogli riprodotti da stampanti, fotocopiatrici e fax.

Utilizzo degli Strumenti dell'Ente e postazioni di lavoro

Strumenti di registrazione degli accessi

Istituzione fa uso di *un foglio presenze mensile*, consegnati esclusivamente al Personale con lo scopo di garantire una corretta analisi dell'orario di lavoro, comprensivo di assenze per malattia, formazione, ferie, permessi e straordinari ai fini dell'erogazione del corrispettivo.

Il foglio presenze è affidato direttamente al singolo Destinatario, che ne risponde a titolo penale e disciplinare.

Postazione di lavoro

Con riferimento alla propria postazione di lavoro, il Personale, al termine dell'orario di lavoro, deve in ogni caso:

- garantire che la postazione di lavoro sia priva di materiale o documenti contenenti informazioni relative ad Istituzione che devono essere conservati in appositi cassetti e/o armadi;
- se previsto, chiudere a chiave cassetti, porte degli uffici o di aree ad accesso limitato;
- raccogliere tutti i documenti stampati e i documenti che non sono più richiesti/necessari e provvedere alla loro definitiva eliminazione.

Internet

Istituzione individua i Destinatari ai quali è consentito l'utilizzo di Internet presso la propria postazione di lavoro, previa identificazione con User ID e Password: anche in considerazione di ciò, è comunque vietato condividere ed utilizzare credenziali di altri utenti, in particolare per accedere ad Internet. Istituzione può altresì consentire l'accesso alla connessione internet aziendale, presso i propri locali, per un uso occasionale, a collaboratori esterni, clienti, e/o terzi non dipendenti, comunque qualificati Destinatari ai sensi del presente Regolamento, e che pertanto saranno tenuti a rispettare le regole di utilizzo ivi indicate.

Al fine di garantire un appropriato utilizzo della rete internet, tutti i Destinatari devono rispettare rigorosamente le seguenti regole:

- l'utilizzo del collegamento aziendale ad internet per la navigazione sul web deve essere finalizzato a scopi esclusivamente lavorativi, ed in ogni caso nel rispetto del rapporto professionale con Istituzione e dei principi generali di liceità, responsabilità e correttezza della condotta;
- è consentita la navigazione su siti contenenti informazioni necessarie o utili all'attività lavorativa o, comunque, all'acquisizione di notizie utili alla propria formazione/informazione professionale;
- non è consentito utilizzare internet provider diversi da quello ufficiale utilizzato da Istituzione;
- non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, posto che in ogni caso la Istituzione ha previamente provveduto a predisporre appositi filtri che bloccano l'accesso ad una serie di siti ritenuti inidonei o pericolosi;

Revisione 01 del

30/06/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

- non è consentito scaricare e/o comunque installare software gratuiti (freeware e shareware) prelevati da siti Internet, se non espressamente autorizzato. È altresì proibito scaricare illecitamente video, testi, immagini, brani musicali, giochi e altri materiali protetti dal diritto d'autore e, comunque, violare in qualunque modo la Legge sul Diritto d'Autore e/o il Codice della Proprietà Industriale (con particolare, ma non esclusivo, riferimento al *know-how* di Istituzione);
- non è consentito lo scambio (ad esempio Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright;
- non è permesso, per motivi non professionali, partecipare a forum, utilizzare chat line o bacheche elettroniche, social network, anche usando pseudonimi;
- tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus;
- i Destinatari si impegnano a non interferire volontariamente con il buon funzionamento dei sistemi informatici e di rete di Istituzione, avendo comunque la responsabilità di segnalare tempestivamente all'indirizzo all'Amministratore di Sistema, la presenza di attività sospette sui propri sistemi o sulla rete.

Una volta cessato il rapporto tra i Destinatari e Istituzione, a qualsiasi titolo e per qualunque ragione, copia del traffico Internet sarà conservata sul server centrale e/o sui *backup* di Istituzione, entro i termini previsti dal presente Regolamento, salvo che vi siano elementi che inducano Istituzione stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Intranet

L'accesso remoto all'intranet aziendale avviene attraverso l'uso di Strumenti dell'Ente forniti da Istituzione o in caso di somma urgenza da dispositivi personali, attenendosi rigorosamente alle norme comportamentali espresse in questo Regolamento. In caso di mancata autorizzazione di utilizzo di dispositivi propri per fattore di urgenza, è fatto divieto di utilizzare un personal computer o altro dispositivo di proprietà o di terzi per effettuare tale accesso.

I servizi di connettività wireless di ogni tipo (ad esempio bluetooth, *wi-fi*), disponibili sugli elaboratori fissi o portatili, sui telefoni e palmari cellulari, per la loro connessione ad altre reti devono essere disabilitati quando connessi alla rete aziendale.

Posta elettronica aziendale

La posta elettronica, messa a disposizione da Istituzione a favore dei Destinatari all'uopo autorizzati, rappresenta uno strumento di esclusiva proprietà aziendale per lo svolgimento di attività lavorative/professionali.

L'utenza di posta elettronica aziendale è strettamente personale ed è pertanto responsabilità di ciascun utente garantire la riservatezza delle credenziali di accesso al servizio nonché il corretto utilizzo dello stesso. Inoltre, possono essere resi disponibili, sulla base di necessità operative/organizzative, indirizzi di posta elettronica per le strutture dell'Ente, ad uso comune, condivisi tra i soggetti assegnati al medesimo servizio (ad esempio, servizi di *helpdesk*). Anche tali indirizzi di posta elettronica sono di esclusiva proprietà aziendale e i Destinatari all'uopo autorizzati condivideranno la responsabilità del loro utilizzo.

Revisione 01 del

30/06/2021

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Per una corretta fruizione del servizio di posta elettronica aziendale, che tuteli i Destinatari e Istituzione, devono essere rispettate le seguenti regole:

- è necessario fare attenzione alla posta ricevuta. Nel caso di mittenti sconosciuti o messaggi insoliti, di dubbia autenticità o provenienza e/o con contenuti non attinenti al lavoro svolto, per non correre il rischio di essere infettati da virus e/o di essere vittima di Phishing, occorrerà contattare l'Amministratore di Sistema e, comunque, cancellare i messaggi senza aprirli. In particolare, non dovranno essere aperti documenti con estensioni diverse da quelle comunemente utilizzate e autorizzate (.doc, .xls, .ppt, .pdf) e/o con nomi "sospetti" e/o "anomali". Qualora, in allegato ad un'e-mail, vi fossero file eseguibili (estensione .exe) è necessario accertarsi preventivamente del loro contenuto, verificando il mittente del messaggio e comunque controllare tutti file in allegato prima del loro utilizzo e non eseguire download di file eseguibili.
- accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima prevista per il destinatario;
- inviare allegati solo nei formati più usati: ad es. *.txt, *.rtf, *.doc, *.ppt, *.xls, *.pdf, *.gif, *.tif;
- non è consentito inviare o memorizzare messaggi di natura oltraggiosa, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, social network o mailing-list, salvo diversa ed esplicita autorizzazione da parte della Istituzione. L'iscrizione ad una mailing list o a servizi simili (chat, forum, social network, ecc.) è consentita solo se funzionale all'attività aziendale e previa autorizzazione del proprio responsabile;
- non è, altresì, consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per inviare messaggi di tipo umanitario, sociale o di solidarietà, salvo diversa ed esplicita autorizzazione rilasciata dal proprio responsabile gerarchico;
- non è consentito utilizzare la posta elettronica per finalità che esulano dall'espletamento delle mansioni affidate a ciascun dipendente;
- non è consentito creare, archiviare o spedire messaggi pubblicitari o promozionali in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto;
- non è consentito inviare messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte;
- non è consentito scaricare sulla propria area di server o sulle risorse condivise in rete file allegati a messaggi di posta elettronica di caselle diverse da quelle assegnate all'utilizzatore;
- la posta elettronica non deve essere utilizzata per ricevere, memorizzare o spedire materiale che violi le norme sul diritto d'autore o proprietà industriale (copyright, marchi, ecc.);
- ogni e-mail inviata deve contenere, come nota finale allegata in automatico, un'adeguata informativa relativa alle informazioni confidenziali.

- Esempio in italiano: "Avvertenza. Questo messaggio (compreso ogni eventuale allegato) è riservato ad uso esclusivo dell'individuo o dell'Ente o soggetto giuridico cui è indirizzato e può contenere informazioni che sono da intendersi come riservate e non destinate a pubblica divulgazione e soggette a tutela legale. Se non siete i destinatari di questo messaggio non dovete farne uso, diffonderlo o estrarne copia, in qualunque forma, né fare affidamento sul suo contenuto. Nel caso in cui Le fosse giunta per errore, La preghiamo di (i) comunicarcelo e (ii) provvedere alla sua distruzione immediata. E' responsabilità del destinatario proteggere i propri sistemi informatici da aggressioni esterne. Questo indirizzo di posta elettronica non è un indirizzo di posta privato e perciò il suo utilizzo è soggetto a regolamentazione. Grazie."

Revisione 01 del

20/09/2014

Dorsaduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Esempio in inglese: "Notice. This message (including any attachments) is intended only for the use of the individual or entity to which it is addressed and may contain information that is non-public, proprietary, privileged, confidential, and exempt from disclosure under applicable law or may constitute as attorney work product. If you are not the intended recipient of this message, you must not use, disseminate or copy it in any form or take any action in reliance of it. If you have received this communication in error, notify us immediately by telephone and (i) destroy this message if a facsimile or (ii) delete this message immediately if this is an electronic communication. Recipient is accountable for his/her system protection from unlawful interference. This email is not a private address; its use is subject to data controller's policy. Thank you";

- è opportuno inserire la propria firma in calce alle e-mail, riportando la direzione e l'unità di appartenenza, secondo le istruzioni ricevute dai propri responsabili;
- quando possibile, inviare gli allegati ai messaggi rivolti a destinatari esterni ad Istituzione in un formato compresso (*.zip, *.rar), al fine di ottenere un messaggio di dimensioni più contenute possibile, riducendo così il rischio di un mancato recapito a causa delle sue dimensioni eccessive;
- sempre per ragioni di contenimento della dimensione dei messaggi, è fortemente sconsigliato inserire immagini o altri file multimediali nel loro corpo o nella "firma";
- è consigliabile effettuare preventivamente una replica in locale di tutte quelle e-mail inviate o ricevute che potrebbero ricoprire un interesse aziendale. Inoltre, gli utenti sono tenuti a mantenere in ordine la propria casella di posta elettronica, cancellando documenti inutili ed e-mail non necessarie, in modo tale da razionalizzare l'impiego delle risorse informatiche e tecnologiche;
- è opportuno scrivere i propri messaggi di posta elettronica in un formato congruente con il programma di posta del destinatario (normalmente il formato di puro testo viene sempre accettato);

Ogni comunicazione interna od esterna, inviata o ricevuta, che abbia contenuti rilevanti o contenga impegni per Istituzione deve essere autorizzata o visionata dal superiore gerarchico.

Infine, si informa che in alcuni casi particolari, su esplicita richiesta delle Autorità competenti (Guardia di Finanza, Autorità Giudiziaria, ecc.), le e-mail memorizzate nei server potrebbero essere eventualmente divulgate o rese note alla stessa.

Nei casi di assenza programmata, il Personale dovrà attivare i sistemi di risposta automatica ("Out of office") disponibili al fine di garantire la continuità del servizio e dovrà indicare il nominativo di un altro utente a cui potrà essere inviata, in copia conoscenza, la propria corrispondenza elettronica. In caso di prolungata assenza od in situazioni di emergenza, i Destinatari potranno attivare tale dispositivo di risposta automatica in riferimento ai rispettivi indirizzi di posta elettronica aziendale.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, i Destinatari potranno delegare un'altra persona (fiduciario) a verificare il contenuto dei messaggi.

Nel caso di cessazione del rapporto di lavoro (subordinato/ di collaborazione o somministrazione, ecc.), al fine di consentire la continuità lavorativa, previa immediata disattivazione dell'account di posta elettronica aziendale, potrà attivare un sistema di risposta automatica che informi i mittenti delle e-mail della disattivazione dell'account di posta elettronica aziendale /o della cessazione del rapporto di lavoro, invitandoli a contattare altro dipendente.

Revisione 01 del

30/01/2014

Dorsoduro 948 - 30123 Venezia - Tel. 041 5280182 - Fax - 041 5280049 - C.F. 00012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Una volta disattivato l'account di posta elettronica, copia dei messaggi di posta elettronica sarà conservata sul server centrale e/o sui *backup* de, entro i termini previsti dal presente Regolamento, salvo che vi siano elementi che inducano Istituzione stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di difesa di un diritto in sede giudiziaria), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Uso personale

L'utilizzo di Internet e/o strumenti di web mail personali durante l'orario di lavoro e/o, comunque, mediante gli Strumenti dell'Ente è consentito soltanto eccezionalmente e occasionalmente, con modi ed entro limiti, temporali e quantitativi, tali da non incidere negativamente sul livello di performance professionale, dei sistemi, dell'organizzazione, o sull'attività lavorativa generale.

In ogni caso, è fatto espresso divieto di usare, anche eccezionalmente, la casella di posta elettronica aziendale per ragioni e/o finalità personali e di inoltrare, in qualunque modo, verso eventuali strumenti di web mail personali, messaggi ricevuti sulla casella di posta elettronica aziendale e/o dati, documenti e/o informazioni della Istituzione.

Software

È opportuno, per garantire la sicurezza del Software messo a disposizione, che i Destinatari rispettino le seguenti regole:

- Istituzione acquista le licenze d'uso dei Software per gli Strumenti dell'Ente da varie realtà esterne, pertanto è soggetta a limitazioni nell'utilizzo di tali programmi e, a meno di una specifica autorizzazione concessa dallo sviluppatore del software, non ha il diritto, e con essa i Destinatari, di riprodurlo, a meno di ragioni di salvataggio (copie di back-up opportunamente documentate);
- per quel che riguarda le applicazioni client/Server e genericamente in rete, i Destinatari sono tenuti a utilizzare i Software loro concessi in uso solo entro i limiti specificati nei relativi contratti di licenza;
- non è consentito riprodurre, adattare, trasformare, distribuire Software in licenza d'uso aziendale;
- come stabilito dalla Legge sul Diritto d'Autore, è assolutamente vietata la duplicazione illegale del software; coloro che violino detta disposizione sono responsabili sia civilmente sia penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione. I Destinatari che effettuano, acquisiscono o usano copie non autorizzate del Software, subiranno le relative sanzioni disciplinari previste, ove applicabili;

È inoltre assolutamente vietato utilizzare e/o installare software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici (a titolo esemplificativo: programmi di *password recovery*, *cracking*, *sniffing*, *spoofing*, *serial codes*, ecc.);

La manutenzione software deve essere svolta solo dal personale autorizzato e competente. Pertanto si raccomanda a tutti i Destinatari di rivolgersi sempre all'Amministratore di Sistema. Nel caso in cui i Destinatari vengano a conoscenza di una qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi, essi dovranno darne tempestivamente comunicazione utilizzando il software denominato "Ticket".

È fatto in ogni caso specifico divieto di modificare gli standard di configurazione dei software installati sul proprio PC.

Revisione 01 del

30/09/2024

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Antivirus

Ogni personal computer viene corredato di software antivirus standard aziendale, adeguatamente configurato ed aggiornato.

È vietato disattivare il software antivirus o modificarne la configurazione. È doveroso collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

I Destinatari che abbiano ricevuto in dotazione Strumenti dell'Ente non possono installare né ulteriori software antivirus, né altri diversi da quelli standard dell'Ente.

I Destinatari devono tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali o di indubbia integrità, ecc.).

Prima di caricare un qualunque tipo di dato o programma da un supporto esterno aziendale (floppy disk, hard disk USB, pen flash USB, cassette magnetiche, CD-ROM, ecc.) i Destinatari devono essere stati preventivamente autorizzati e procedere alla scansione del supporto utilizzando l'antivirus messo a disposizione. Nel caso venga rilevato un virus non eliminabile dal software antivirus, i Destinatari non devono utilizzare il dispositivo infetto.

Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, i Destinatari devono immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto.

Limitazioni al sistema di crittografia

È proibito cifrare le informazioni, nonché trasmettere, salvare o ricevere informazioni cifrate, salvo i casi in cui si ottenga preventiva autorizzazione o vi siano disposizioni operative che ne richiedano l'esecuzione, regolamentandone le relative modalità nei casi previsti (es. per la protezione dei dati personali).

Telefoni / tablet

I telefoni, fissi e/o *mobile*, e i *tablet* sono eventualmente affidati ai Destinatari al solo fine di rendere la prestazione lavorativa e devono essere utilizzati secondo le modalità indicate nel presente paragrafo. È fatto quindi divieto di un cd. "uso promiscuo" e, pertanto, l'utilizzo di queste apparecchiature ai fini privati è consentito solo in caso di comprovata necessità o urgenza; in tal caso il Dipendente sarà ritenuto esclusivo responsabile per ogni eventuale danno che dovesse derivare da detto utilizzo privato.

Inoltre, con particolare riferimento agli eventuali telefoni *mobile* / *tablet*, è altresì fatto espresso divieto di:

- evitare di chiamare numeri a pagamento, salva preventiva autorizzazione scritta del diretto superiore;
- proteggere tutti i dati presenti nel dispositivo, anche mediante cd. "pin code" (o strumenti analoghi), sistemi di blocco automatico dello schermo e cifratura;
- evitare di scaricare e/o installare applicazioni non preventivamente autorizzate che, comunque, che non siano coerenti con l'esclusivo utilizzo lavorativo del telefono;

In ogni caso, qualora la sicurezza dei dati presenti sul telefono *mobile* / *tablet* sia insindacabilmente ritenuta a rischio da parte di Istituzione (e.g. in caso di smarrimento, e/o alla luce di bug e/o notizie di possibili breach ecc.), quest'ultima potrà intervenire, anche da remoto, sugli Strumenti dell'Ente. A tal fine, i telefoni *mobile* / *tablet* dovranno sempre essere configurati in modo tale da consentire la ricezione di una richiesta remota di cancellazione dei dati ivi contenuti.

Revisione 01 del

30/08/2024

Dorsoduro 945 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Controlli da parte di Istituzione

In relazione agli Strumenti dell'Ente, Istituzione si riserva la facoltà di effettuare controlli saltuari e occasionali per verificare l'integrità del sistema informatico, l'uso equilibrato e conforme all'attività ed alle politiche dell'Ente degli Strumenti dell'Ente e per l'ordinaria manutenzione degli stessi, nonché per tutte le finalità connesse al rapporto di lavoro, riservandosi, in ogni caso, di accertare e segnalare tempestivamente eventuali abusi/violazioni commessi dai Destinatari.

In ogni caso viene garantito ai Destinatari il rispetto dei principi di liceità, pertinenza e non eccedenza previsti dalla Normativa Applicabile, nell'effettuazione di eventuali controlli, nonché il rispetto del divieto dei controlli a distanza dei lavoratori dipendenti.

Per le suddette ragioni, Istituzione si riserva di monitorare le reti e tutti gli altri Strumenti dell'Ente, in particolare, nei seguenti casi:

- necessità di effettuare verifiche sulla funzionalità e sulla sicurezza dei sistemi;
- constatazione di utilizzo indebito della posta elettronica;
- necessità di effettuare verifiche tese alla protezione del patrimonio;
- presenza di casi di abusi da parte di singoli o reiterati;
- presenza di indizi relativi alla fuga di informazioni riservate o confidenziali.

Segnatamente, controlli periodici possono essere effettuati su:

- il volume dei messaggi scambiati;
- la durata dei collegamenti ad Internet (globale, per funzione, per gruppi o tipologia di utenti);
- le informazioni raccolte dai dispositivi di sicurezza (Firewall, Antivirus, IDS, IPS, ecc.).

Le modalità con cui verranno effettuati i controlli saranno le seguenti:

- i controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Destinatari, su dati aggregati e anonimi tramite l'analisi di statistiche generali;
- successivamente, verranno inoltrati avvisi collettivi di diffida al compimento di operazioni non consentite o, a seconda della gravità, verranno prese misure di tipo individuale, specialmente in caso di abuso e/o anomalie reiterate;
- nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare i dati registrati con riferimento all'esercizio o alla difesa di un diritto in sede giudiziaria (azioni da parte di terzi verso Istituzione o viceversa, o in caso di verifiche relative ad un presunto comportamento illecito), oppure si ottemperi all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria, tale periodo verrà prolungato secondo le necessità del caso e nel pieno rispetto delle finalità descritte;
- in ogni caso verranno esclusi controlli prolungati, costanti o indiscriminati o comunque preordinati al controllo a distanza dei lavoratori.

A tal riguardo si precisa che:

- in ogni caso non si fa luogo alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail ivi inclusi i salvataggi periodici dei dati (c.d. "back up");
- inoltre, non si procede alla riproduzione o memorizzazione sistematica delle pagine web visualizzate dall'Utente, né alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo né all'analisi occulta dei computer portatili affidati in uso.

Revisione 01 del

30/09/2024



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza, sia sul PC dei Destinatari che sulle unità di rete. L'effettuazione di tali controlli, che non hanno lo scopo di monitorare l'attività dei Destinatari, bensì di verificare la sicurezza del sistema e per effettuare la manutenzione, avverranno nel pieno rispetto della Normativa Applicabile.

Con particolare riferimento all'utilizzo dei telefoni dell'Ente, Istituzione effettua verifiche periodiche volte a verificare la coerenza dei costi derivanti dalle utenze telefoniche associate con i suddetti apparecchi, nel pieno rispetto della Normativa Applicabile; a tal proposito verranno segnalati ai Destinatari eventuali discrepanze o problemi che dovessero essere riscontrati nel corso di tali controlli.

Di tali controlli e del relativo trattamento dati è stata fornita informativa ai Destinatari con il presente Regolamento, anche ai sensi dell'art. 13 del GDPR; l'eventuale conservazione di tali dati avverrà per il tempo strettamente limitato al perseguimento lecito di finalità organizzative, produttive e di sicurezza.

Il mancato rispetto o la violazione delle regole contenute nel Regolamento è perseguibile con provvedimenti disciplinari previsti dal CCNL, ed altresì con le azioni civili e penali previste dalle leggi vigenti, qualora si verificano gli estremi per la sussistenza della responsabilità civile o penale.

Istituzione non effettua alcun controllo illegittimo o indiscriminato sull'utilizzo di internet e della posta elettronica da parte dei Destinatari. In particolare, Istituzione non effettuerà alcun controllo generalizzato e sistematico del contenuto dei profili *social network* del Personale, salvo che ciò sia necessario per il perseguimento di un legittimo interesse (quale, ad esempio, la verifica del rispetto di un patto di non concorrenza, o fattispecie analoghe) e/o per verificare il rispetto del Regolamento e/o, comunque, qualora vi siano fondati sospetti di possibili condotte illecite e/o di un possibile pregiudizio al patrimonio e/o all'immagine di Istituzione.

Le informazioni raccolte consentono un controllo dell'efficienza e dell'utilizzo corretto degli Strumenti dell'Ente e del Network. I controlli non sono finalizzati al controllo a distanza delle attività lavorative del Personale (salvo eventuale esplicita richiesta in tal senso da parte delle Autorità competenti, oppure salvo che vi siano fondati sospetti di una condotta illecita e/o di un possibile pregiudizio al patrimonio e/o all'immagine aziendale). In particolare, la Istituzione non adotta alcuno dei seguenti mezzi:

- lettura e registrazione sistematica dei messaggi di posta elettronica dei dipendenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire il servizio di Posta elettronica;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visitate;
- lettura e registrazione di caratteri inseriti tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- analisi occulta dei dispositivi per l'accesso ad Internet o l'uso della posta elettronica aziendale.

I sistemi preposti alla gestione di internet, della posta elettronica e della rete interna aziendale registrano, su appositi file di sistema detti file di LOG, una serie di informazioni aggregate, in modo da non poter essere ricondotti all'utente che li ha generati.

Ove possibile, i dati sono acquisiti in modalità anonima e quindi non riconducibili direttamente all'identità dei singoli Destinatari che li hanno generati. Tali dati saranno archiviati, con le opportune misure di sicurezza e riservatezza, ed eventualmente controllati nei limiti sanciti dalla normativa vigente e dal presente Regolamento [nonché dalla Retention Policy], fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano Istituzione stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Revisione 01 del

30/09/2024



Dorsoduro 948 - 30123 Venezia - Tel. 041 5269182 - Fax - 041 5260049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it

ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Conservazione

I file di LOG contengono le informazioni relative ad almeno gli ultimi 180 giorni.

I dati contenuti nei LOG possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia giudiziaria e/o dell'autorità giudiziaria;
- allorquando sia necessario un intervento – espressamente richiesto dall'utente – volto al recupero di dati contenuti in file o e-mail accidentalmente andati persi.

Quotidianamente vengono salvati, su supporto esterno, tutti i dati relativi a:

- cartelle di rete;
- posta elettronica;
- file di LOG.

I supporti esterni, conservati per almeno 180 giorni, possono essere accessibili solo agli Amministratori di Sistema.

Il contenuto dei dispositivi di memorizzazione degli Strumenti dell'Ente, delle cartelle dei *file server*, degli *account* di posta elettronica aziendale saranno conservati sul server centrale e/o sui *backup* della Istituzione per dieci anni, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano la Istituzione stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Il traffico internet sarà cancellato da Istituzione periodicamente, ogni dodici mesi, fatte salve eventuali esplicite richieste delle Autorità competenti e/o salvo che vi siano elementi che inducano Istituzione stessa a ritenere necessario un periodo di conservazione più lungo (ad esempio, per finalità di giustizia), anche in seguito ad un'eventuale valutazione di impatto ai sensi e per gli effetti dell'art. 35 del GDPR.

Altri Strumenti dell'Ente

Istituzione fa uso anche di altri strumenti utilizzati dai Lavoratori per rendere la prestazione lavorativa, quali:

- sistema di videoconferenze;

I suddetti apparati e software sono strumenti di lavoro e devono essere utilizzati esclusivamente per motivi connessi all'esecuzione della prestazione di lavoro, anche nel rispetto dei principi di economia.

Istruzioni in caso di cessazione del rapporto di lavoro o di collaborazione

Fermo quanto previsto dai paragrafi precedenti e, in particolare, *sub 0*, in caso di cessazione del rapporto di lavoro o di collaborazione e in tutti i casi in cui ciò sia richiesto dalla Istituzione (quali ad esempio il venir meno delle ragioni di servizio che avevano determinato l'assegnazione, la sua sostituzione con altro Strumento Aziendale), gli Strumenti dell'Ente dovranno essere restituiti senza cancellare alcun dato aziendale ivi memorizzato, da intendersi sin d'ora di esclusiva proprietà di Istituzione, avendo cura i Destinatari di eliminare preventivamente soltanto tutti i propri eventuali dati, nonché le eventuali informazioni e comunicazioni, personali non attinenti l'attività lavorativa svolta che gli stessi abbiano eventualmente archiviato negli Strumenti dell'Ente in dotazione, in tal caso violando quanto previsto dal presente Regolamento.

Revisione 01 del

30/04/2024

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it
PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Più in dettaglio, nell'ipotesi di cui al precedente paragrafo, i dati custoditi dai Destinatari afferenti gli Strumenti dell'Ente dovranno, comunque, essere restituiti integralmente ad Istituzione, secondo quanto previsto dalla lettera di designazione tra i "Soggetti Autorizzati al Trattamento" con espresso divieto di conservarli, duplicarli, comunicarli o diffonderli. Quando il rapporto di lavoro o collaborazione con il Lavoratore venga a cessare, i dati, le informazioni, i file e archivi di lavoro inerenti l'attività lavorativa / professionale svolta dallo stesso, inclusi quelli riportati o allegati nelle e-mail, devono essere senz'altro restituiti ad Istituzione, la quale è tenuta a conservare questi dati ed informazioni solo a fini inerenti la gestione aziendale senza duplicare, comunicare o diffondere alcun dato personale.

Violazioni e sanzioni

Le Istruzioni contenute nel presente Regolamento hanno valore di normativa aziendale e la loro violazione può comportare l'applicazione di sanzioni disciplinari previste dal CCNL.

La non ottemperanza delle suddette disposizioni potrà determinare l'applicazione da parte della Istituzione di restrizioni considerate appropriate, nonché, da l'applicazione da parte della stessa:

- dei provvedimenti disciplinari a carico del Personale, previsti dal regolamento aziendale e dal CCNL;
- della risoluzione del contratto e delle azioni civili e penali stabilite dalla legge, nei confronti dei collaboratori.

Osservanza delle disposizioni in materia di protezione dei dati personali

È, in ogni caso, obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali e di misure minime di sicurezza, come indicato nella lettera di nomina a "Soggetti Autorizzati al Trattamento" nonché alle istruzioni fornite dalla Istituzione.

Entrata in vigore del Regolamento e pubblicità

Il presente Regolamento entrerà in vigore il

Copia del presente Regolamento sarà distribuita tramite e-mail a ciascun Dipendente e sarà affisso nella bacheca.

LAVORO DA REMOTO (SMART WORKING, TELELAVORO)

5.3.1. Fermo quanto previsto da

- a) l'Accordo sullo smart working sottoscritto tra l'Ente e le OO.SS, ovvero con il singolo dipendente, in tutti i casi in cui il rapporto di lavoro subordinato venga eseguito mediante la modalità c.d. di *smart working*, disciplinata dagli artt. 18 e seguenti della L. n. 81/2017 (ovvero in ogni caso di eventuale attività lavorativa svolta da remoto, in conseguenza di situazioni emergenziali) (lo "*Smart Working*") o da
- b) l'Accordo Interconfederale del 9 giugno 2004 per il recepimento dell'accordo quadro europeo sul telelavoro del 16 luglio 2002, inteso come "una forma di organizzazione e/o di svolgimento del lavoro che si avvale delle tecnologie dell'informazione nell'ambito di un contratto o di un rapporto di lavoro, in cui l'attività lavorativa, che potrebbe anche essere svolta nei locali dell'impresa, viene regolarmente svolta al di fuori dei locali della stessa" (il "*Telelavoro*"),

Revisione 01 del

22/09/2024

Dorsoduro 948 - 30123 Venezia - Tel. 041 5289182 - Fax - 041 5280049 - C.F. 80012150274

www.istituzioneveneziana.it - info@istituzioneveneziana.it

PEC: responsabile.servizio@pcert.postecert.it



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

Nel caso in cui la prestazione lavorativa sia svolta in *Smart Working* ovvero *Telelavoro* (congiuntamente il "**Lavoro da remoto**") il Personale deve rispettare le seguenti regole:

- 1) l'accesso remoto alla Rete Aziendale deve avvenire esclusivamente attraverso l'uso degli Strumenti dell'Ente e nel rispetto delle norme comportamentali stabilite in questo Regolamento;
- 2) è fatto, pertanto, divieto di utilizzare un PC o altro dispositivo di proprietà o di terzi per effettuare tale accesso, salvo che ciò non sia stato espressamente autorizzato dalla Funzione IT previa verifica dell'adeguatezza del dispositivo di proprietà o di terzi secondo le regole di sicurezza dell'Ente.

5.3.2. Per consentire al Personale di eseguire la propria prestazione lavorativa attraverso gli Strumenti dell'Ente anche con le modalità del Lavoro da remoto, l'Ente mette a disposizione degli stessi le seguenti risorse:

- a) accesso via web da remoto con modalità sicure;
- b) accesso remoto "terminalizzato" (es. citrix) che consenta l'elaborazione e visualizzazione di una sessione di lavoro in sicurezza all'interno dell'ambiente informatico dell'Ente;
- c) VPN ovvero un canale tra il dispositivo remoto e l'Ente attraverso il quale si acceda direttamente agli applicativi e ai dati ivi contenuti;
- d) strumenti di web-meeting per supportare sia l'organizzazione del lavoro all'interno dell'Ente con lo scopo di svolgere in modalità remota incontri e riunioni con i colleghi, sia i contatti con il personale esterno all'Ente (ad esempio, clienti e fornitori).

5.3.3. Il Personale è altresì informato su:

- a) le modalità per deviare le chiamate dal telefono dell'Ente allo smartphone sono ;
- b) le modalità per disattivare la deviazione di chiamata;
- c) le istruzioni operative per poter effettuare videocall interne ed esterne utilizzando gli strumenti di web-meeting;

5.3.4. Ove la connessione dati non sia fornita dall'Ente il Personale è tenuto a:

- 1) utilizzare una connessione a Internet privata di proprietà personale, ferma la possibilità di utilizzare il telefono cellulare eventualmente consegnato come *hotspot* in assenza di connessione; in tale ultimo caso, gli utenti non potranno superare il traffico dati mensile consentito che dovrà risultare sufficiente ai fini dell'ordinario utilizzo del dispositivo mobile.
- 2) per un utilizzo sicuro della connessione privata di proprietà personale,
 - a) aggiornare il firmware del modem-router all'ultima versione disponibile;
 - b) modificare la *Password* di accesso al proprio router. Se la *Password* è la stessa dall'acquisto del router ovvero trattasi di *Password* non particolarmente complessa, è necessario modificarla con una complessa;
 - c) modificare la *Password* di accesso al WiFi se ci si connette ad un modem router wireless.
- 3) non fare ricorso ad una rete di connessione pubblica, salvo in casi eccezionali (ad esempio indisponibilità temporanea della rete privata) e sempre a condizione che la rete pubblica prescelta sia di comprovata sicurezza o affidabilità. A tal riguardo si raccomanda di prediligere connessioni ricollegabili ad un soggetto identificabile come sicuro es. gli hotspot di provider noti, la rete pubblica comunale ecc.. ovvero che richieda forme di autenticazione e/o *Password* per l'accesso.

Revisione 01 del

30/09/2021



ISTITUZIONE VENEZIANA

SERVIZI SOCIALI ALLA PERSONA

5.3.5. I Destinatari dovranno prediligere al massimo l'utilizzo di documenti digitali ed evitare, quale regola generale, i documenti cartacei, salvo che l'utilizzo degli stessi sia strettamente necessario; in questo caso dovranno essere rispettate le seguenti istruzioni:

1. predisporre copie degli originali, utilizzare solo le copie di questi ultimi e non portare in nessun caso gli originali al di fuori dei locali dell'Ente;
2. limitare allo stretto indispensabile la quantità di documenti cartacei da portare al di fuori dei locali dell'Ente;
3. prestare particolare attenzione alla protezione e alla custodia dei documenti cartacei durante il trasporto dai locali dell'Ente ai luoghi extra dell'Ente, evitando la loro esposizione a terzi e avendo cura di prevenire eventuali furti o smarrimenti; in particolare, conservare in armadi/cassettiere protette da serratura gli eventuali documenti dell'Ente cartacei portati al di fuori dai locali dell'Ente;
4. distruggere le copie dei documenti cartacei se non più necessari, salvo diversa istruzione o che non vi siano ulteriori ragioni di conservazione e/o archiviazione, avendo cura di renderli non facilmente riconoscibili (es. sminuzzando la documentazione; anonimizzando i dati personali ecc.).

ISTITUZIONE VENEZIANA
Il Segretario Direttore
Dott. Marino Favaretto

Revisione 01 del

30/09/2024

