Politiche ed utilizzo delle risorse informatiche

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Approvato con delibera del CN del 30/10/2020

Ver. 01

Finalità della Policy

Le finalità di questo documento sono:

1. garantire e salvaguardare la sicurezza e la privacy degli utenti abilitati dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (in seguito CNDCEC);

2. stabilire una policy per la sicurezza e il rispetto della privacy nell'utilizzo delle risorse informatiche dell'Ente con riferimento in particolare alle misure di sicurezza imposte dalle normative per il trattamento di dati personali;

3. fornire idonee indicazioni ed istruzioni agli utenti interessati dalle predette misure di sicurezza;

4. regolamentare l'utilizzo delle risorse informatiche dell'Ente in modo che siano utilizzate in maniera efficace, produttiva e orientata al raggiungimento degli obiettivi dell'Ente;

5. garantire la sicurezza e prevenire il danneggiamento delle risorse informatiche dell'Ente.

Campo di applicazione

Questa policy si applica:

1. a tutte le risorse informatiche di proprietà del CNDCEC e/o messe a disposizione;

2. a tutte le operazioni di accesso a informazioni registrate ed archiviate elettronicamente tramite risorse informatiche dell'Ente;

3. a tutte le forme di comunicazione operate attraverso la rete del CNDCEC e la posta elettronica;

4. a tutti i dati del CNDCEC visualizzati o elaborati anche con dispositivi personali.

Destinatari

Il regolamento si applica a tutti i dipendenti a tempo pieno o parziale (senza alcuna distinzione di ruolo e/o livello), collaboratori, consulenti, consiglieri, dipendenti di società o aziende esterne legate da contratti di fornitura e/o di servizi o altri individui in possesso di specifiche credenziali di autenticazione alla quale è consentito l'utilizzo dell'accesso alle risorse dell'Ente (a prescindere dal tipo di rapporto contrattuale intrattenuto con l'Ente).

Entrata in vigore del regolamento e diffusione

Il regolamento entra in vigore con delibera del CN.

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalla presente.

Ai fini dell'esercizio del regolamento, si darà adeguata pubblicità mediante invio ai responsabili del trattamento, ai dipendenti, collaboratori e consiglieri e si provvederà alla pubblicazione dello stesso sul sito internet del CNDCEC.

Verifiche

Le segnalazioni di eventuali violazioni devono essere repentinamente comunicate al responsabile di area, che laddove necessario provvederà ad attivare le idonee procedure di verifica con gli Amministratori di sistema del CNDCEC. Non sono ammesse segnalazioni di violazioni in forma anonima. Viene comunque tutelato dall'Ente il diritto alla privacy degli utenti che comunicassero dette violazioni nei limiti previsti dalla normativa italiana.

Sanzioni

Poiché in caso di violazioni contrattuali e giuridiche, sia il CNDCEC sia il singolo utente sono potenzialmente perseguibili con sanzioni anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del sistema informativo. In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali. Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle autorità competenti.

Indicazioni generali

1. L'utilizzo delle risorse informatiche messe a disposizione dal CNDCEC è riservato ai dipendenti dell'Ente e ad altri soggetti espressamente autorizzati dal responsabile di area.

I responsabili delle aree richiedono ai Sistemi Informativi l'abilitazione ai servizi informatici e l'accesso ai software necessari a ciascun utente. Il responsabile di area comunica immediatamente qualsiasi modifica relativa all'organico del servizio che richieda l'attivazione o la sospensione di servizi informatici o autorizzazioni all'accesso ai software (es. cambio di mansioni e/o trasferimento altro ufficio);

2. le risorse informatiche del CNDCEC sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente lavorativi. Ciò vale sia per le risorse condivise (risorse di rete, spazi cloud, stampanti di rete, ecc.), sia per quelle affidate al singolo dipendente (desktop, notebook, smartphone, periferiche, stampanti, ecc.). Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza. L'utilizzo di risorse informatiche del CNDCEC non deve compromettere la sicurezza e la riservatezza del sistema informativo oltre a non pregiudicare ed ostacolare le attività dell'Amministrazione o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici;

3. le risorse informatiche dell'Ente affidate al singolo utente (es. dispositivi e relativi programmi e/o applicazioni) sono strumenti di lavoro appartenenti al patrimonio del CNDCEC e pertanto vanno custoditi in modo appropriato. Il furto, il danneggiamento o lo smarrimento di tali strumenti devono essere prontamente segnalati all'Ente (e qualora necessario denunciato alle competenti autorità). Il dispositivo è assegnato ad un

utente. In caso di trasferimento dell'utente le risorse informatiche debbono esser riconsegnate all'ufficio consegnatario dei beni;

4. le postazioni di lavoro devono essere spente ogni sera prima di lasciare gli uffici. Casi particolari, in cui ci sia la necessità di lasciare sempre attiva la postazione, devono essere esplicitamente autorizzati dal responsabile di area. 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 uso. Qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad eseguire una delle seguenti operazioni: spegnimento, blocco (digitando per es. i tasti CRTL+ALT+CANC) o disconnessione della postazione di lavoro. In caso di inattività prolungata la connessione dell'utente potrà essere sospesa e disconnessa in automatico;

4. Nel caso di computer portatili o smartphone dell'Ente inoltre:

1) L'utente deve custodire con diligenza il dispositivo sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro;

2) se il dispositivo è utilizzato all'esterno (convegni, conferenze ecc.), in caso di allontanamento, deve essere custodito in un luogo protetto;

3) il dispositivo non deve essere mai lasciato incustodito.

Configurazioni dei dispositivi dell'Ente e collegamento alla rete del CNDCEC

1. Non è consentita la modifica delle configurazioni impostate di default sul dispositivo;

2. ogni computer del CNDCEC deve obbligatoriamente essere collegato alla rete del CNDCEC e non può per nessun motivo essere scollegato da tale rete. Casi particolari in cui il computer non debba essere connesso alla rete del CNDCEC devono essere esplicitamente autorizzati dal responsabile di area;

3. per ragioni di sicurezza non è concesso connettere alla rete del CNDCEC stazioni di lavoro private e sistemi di connessione (es. modem, switch, hub ecc.) se non su esplicita e formale autorizzazione dei sistemi informativi.

Installazione di hardware e software

1. Non è consentita l'installazione di programmi provenienti dall'esterno dell'Ente salvo previa autorizzazione del responsabile di area e dei Sistemi Informativi. L'installazione autonoma di software non autorizzato comporta un grave pericolo di introduzione di virus informatici e/o di alterazione della stabilità delle applicazioni presenti nell'elaboratore;

2. non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal CNDCEC su indicazione dei responsabili di area e dei Sistemi Informativi;

3. non è consentita l'installazione autonoma di alcun dispositivo di comunicazione o altro (es. modem, masterizzatori, ecc.), se non con l'autorizzazione esplicita dei responsabili di area e dei Sistemi Informativi;

4. non sono consentiti l'installazione autonoma e/o l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare, criptare o sopprimere il contenuto di comunicazioni e/o di documenti informatici con finalità omissive e fraudolente.

Supporti di memorizzazione

1. Non è consentito l'utilizzo di cd, dvd, nastri magnetici, chiavette USB, hard disk esterni, ecc. di provenienza ignota o dubbia;

2. ogni dispositivo di memorizzazione di provenienza esterna al CNDCEC dovrà essere verificato mediante il programma antivirus prima del suo utilizzo;

3. non è consentito scaricare file provenienti da Internet oppure contenuti in supporti di memorizzazione che non abbiano una chiara attinenza con la propria prestazione lavorativa;

4. i supporti di memorizzazione quali: dvd, nastri magnetici, chiavette USB, hard disk esterni, ecc. contenenti dati del CNDCEC devono essere ridotti a casi di necessità e custoditi in archivi chiusi a chiave;

5. i supporti di memorizzazione contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato anche dopo la cancellazione mediante l'utilizzo di specifici strumenti di recupero dati;

6. non è consentita la memorizzazione e la diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Stampa su stampanti di rete

Si raccomanda agli utenti di prestare la massima attenzione nella stampa soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone. Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato. La stampa di documenti informatici dovrà essere limitata all'attività lavorativa e in ogni caso per documenti per cui esiste l'assoluta necessità di disporre della copia cartacea. In particolare per motivi di economicità per quanto riferito alle stampe a colori.

Scansione su multifunzione

Scansione da multifunzione con invio a casella di posta elettronica:

1. Le scansioni devono essere inoltrate alla propria mail con dominio@commercialisti.it per verificarne la corretta scansione. Solo dalla propria casella mail sarà possibile procedere all'inoltro a una persona terza.

2. È proibito l'invio di scansioni da multifunzione verso mail esterne.

Scansione da multifunzione con salvataggio su cartella di rete:

1. Qualora il file derivante da scansione venga salvato su una cartella condivisa, che sia personale o di gruppo, l'utente si fa carico di spostare il file nel più breve tempo possibile.

2. La cartella condivisa nella quale vengono salvate le scansioni viene automaticamente cancellata periodicamente. La cancellazione periodica non dispensa tuttavia l'utente dall'obbligo di cancellare/spostare le scansioni eseguite dalla cartella condivisa nel più breve tempo possibile (al fine di non rendere

accidentalmente noto a terzi il contenuto dei file scansione). Si raccomanda di porre la massima attenzione nella scansione di documenti contenenti dati personali e sensibili.

Credenziali per l'accesso ai dispositivi e alla rete CNDCEC

Per accedere a dispositivi e alla rete del CNDCEC, l'utente dovrà attenersi al presente regolamento.

1. L'accesso ai dispositivi e alla rete CNDCEC avviene mediante una utenza e una parola chiave segreta (password). La coppia di informazioni prende il nome di credenziali di accesso;

2. dovranno essere adottate le necessarie cautele per garantire la segretezza delle credenziali;

3. la password di accesso alla rete ha in genere un periodo di validità limitato. A intervalli regolari verrà quindi richiesto all'utente di modificare la password;

4. le credenziali di accesso ai dispositivi e alla rete del CNDCEC vengono attribuite dai Sistemi Informativi, all'assunzione del dipendente/inizio del rapporto di collaborazione (ove autorizzato) e devono essere obbligatoriamente modificate al primo accesso;

5. le credenziali vengono immediatamente revocate/annullate dai Sistemi Informativi, alla cessazione del rapporto di dipendenza/collaborazione con il CNDCEC, tramite comunicazione email da parte del responsabile di area;

6. le credenziali di accesso ai dispositivi e alla rete attribuite dai Sistemi Informativi, sono in genere modificabili in totale autonoma dall'utente;

7. l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dall'amministratore di sistema;

8. l'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla rete, consapevole che la cessione delle stesse consente ad altri l'accesso e l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione / modifica di dati;

9. la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che del CNDCEC, di fatti e atti illeciti, con particolare riferimento all'immissione in rete di contenuti critici o contrari all'ordine pubblico o al buon costume così come definiti dalla giurisprudenza corrente;

10. non sono previsti accessi anonimi o di gruppo: laddove questi siano attualmente attivi saranno progressivamente dismessi;

11. è assolutamente proibito l'accesso alla rete locale e/o alle applicazioni condivise con nomi utente diversi da quello assegnato;

12. l'utente si impegna a modificare tempestivamente la password d'accesso alla rete qualora tale dato sia stato rubato, smarrimento, perso o sia noto a terzi;

13. in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto ai Sistemi Informativi;

14. nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al responsabile dell'ufficio;

15. Il CNDCEC si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

Credenziali per l'accesso ai servizi e applicativi dell'Ente

1. Dovranno essere adottate le necessarie cautele per garantire la segretezza delle credenziali e la diligente custodia dei dispositivi eventualmente in possesso ad uso esclusivo a scopo d'autenticazione (quali ad esempio: smart card, braccialetti, dispositivi RFID);

2. la password di accesso agli applicativi ha in genere un periodo di validità limitato. A intervalli regolari verrà quindi richiesto all'utente di modificare la password;

3. le credenziali di accesso ai servizi e applicativi del CNDCEC vengono attribuite/revocate/modificate dall'ufficio gestore dell'applicativo o del servizio su apposita richiesta dei responsabili di area;

4. le credenziali vengono immediatamente revocate/annullate, alla cessazione del rapporto di dipendenza/collaborazione con il CNDCEC non appena ne venga a conoscenza (tramite comunicazione email da parte dell'ufficio del personale o dal responsabile di area);

5. le credenziali di accesso a servizi e applicazioni attribuite, sono in genere modificabili in totale autonoma dall'utente;

6. l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dall'amministratore di sistema;

7. l'utente si impegna a non cedere a terzi le proprie credenziali di accesso a servizi e applicazioni consapevole che la cessione delle stesse consente ad altri l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione / modifica dei dati;

8. la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione a servizi e applicazioni sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che del CNDCEC, di fatti e atti illeciti;

9. non sono previsti accessi anonimi o di gruppo;

10. qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad uscire dall'applicazione o dal servizio (quantomeno la postazione deve essere bloccata);

11. è assolutamente proibito l'accesso ad applicazioni e servizi con nomi utente diversi da quello assegnato;

12. l'utente si impegna a modificare tempestivamente la password d'accesso a servizi e applicazioni qualora tale dato sia stato rubato, smarrimento, perso o sia noto a terzi;

13. in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto al responsabile di area;

14. nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al responsabile dell'ufficio;

15. Il CNDCEC si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

Cartelle condivise

1. Per gli uffici/settori del dominio del CNDCEC è previsto, previa richiesta ai sistemi informativi e al responsabile di area, un sistema di salvataggio dei file su piattaforme cloud (Sharepoint):

a. I documenti salvati sul sito padre CNDCEC di Sharepoint sono tutelati da perdite mediante procedure di salvataggio. La memorizzazione avviene a seconda del grado di riservatezza del documento su cartelle con adeguato livello di condivisione. I livelli di condivisione/privilegi di lettura e scrittura delle cartelle vengono definiti dal/dai responsabile/i della/e struttura/e proprietaria/e delle cartelle stesse e pertanto dei documenti ivi contenuti;

b. Altre piattaforme cloud per lo scambio dati e per il lavoro in modalità agile. Queste modalità permettono lo scambio di file tra utenti e il lavoro in modalità agile (Onedrive) ma non sono soggetti a procedure di copia di riserva.

2. entrambi i sistemi sono aree di condivisione e salvataggio di informazioni inerenti l'attività istituzionale e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file non legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;

3. I Sistemi Informativi si riservano la facoltà di procedere alla rimozione di qualsiasi file o applicazione memorizzata nelle unità di rete qualora ritenuti pericolosi per la sicurezza del sistema;

4. costituisce buona regola la periodica (almeno mensile) cancellazione dagli archivi/cartelle di file obsoleti e/o documenti non più necessari all'attività d'ufficio;

5. L'utente si impegna a non cedere a terzi le proprie credenziali di accesso alle proprie cartelle condivise consapevole che la cessione delle stesse consente ad altri l'utilizzo/accesso a contenuti riservati e la possibilità di cancellazione e modifica degli stessi.

Diritti di accesso e controllo remoto

1. Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, i Sistemi informativi possono avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale;

2. l'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire solo previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso;

3. in caso di malfunzionamenti straordinari e in situazioni di emergenza, i Sistemi Informativi hanno facoltà in qualunque momento di accedere a qualunque sistema informativo del CNDCEC per l'espletamento delle proprie funzioni. I Sistemi Informativi possono in qualunque momento procedere alla rimozione di qualsiasi file o applicazione che riterranno essere pericolosa per la sicurezza, sia sulle postazioni degli utenti che sulle unità di rete o in cloud.

Utilizzo della rete Internet e dei relativi servizi

Regole di utilizzo di internet nelle sedi dell'Ente

1. L'abilitazione alla navigazione su internet è accordata, di norma, a tutti gli utenti del CNDCEC;

2. qualora l'utente non fosse stato abilitato alla navigazione in internet è fatto divieto assoluto di connettersi autonomamente alla rete internet;

3. è vietato modificare le impostazioni di connessione stabilite dai Sistemi Informativi (firewall, IP, proxy ecc.);

4. il sistema di navigazione per mezzo di proxy del CNDCEC effettua il filtraggio dei siti visitati;

5. gli utenti sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web. L'utente è tenuto nel corso della navigazione a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online;

6. per ragioni di sicurezza non è concesso installare software scaricato dalla rete. Eventuali necessità dovranno essere appositamente concordate i Sistemi Informativi.

7. è vietato lo scarico di file audio e video, l'utilizzo di streaming (e in generale tutti gli utilizzi in grado di degradare le prestazioni offerte dal servizio di rete) a meno di utilizzi strettamente attinente l'attività istituzionale;

8. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

9. I Sistemi Informativi hanno facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi dell'Ente;

10. è vietato l'utilizzo di internet a scopi personali non attinenti l'attività istituzionale quali a titolo d'esempio: la partecipazione a forum, l'utilizzo di chat-line, bacheche elettroniche e servizi di rete sociale, la registrazione in guest-book anche utilizzando pseudonimi (nickname), l'adesione a servizi gratuiti di social networking e microblogging, remote banking, acquisti online e simili.

Posta elettronica Casella di posta elettronica del CNDCEC

1. All'atto dell'assunzione/inizio di collaborazione viene assegnato una casella di posta elettronica del CNDCEC nominativa al dipendente/collaboratore (ove autorizzato);

2. all'atto della cessazione del rapporto di dipendenza/collaborazione con il CNDCEC la casella mail viene bloccata e cancellata;

3. l'amministratore di sistema per comprovati motivi può revocare/cancellare la casella di posta elettronica del CNDCEC nominativa di un dipendente / collaboratore;

4. IL CNDCEC favorisce l'utilizzo di indirizzi istituzionali condivisi, o di gruppi di distribuzione, accessibili a più utenti per la consultazione di corrispondenza d'interesse comune a più utenti operanti nei vari uffici/settori. Le persone che condividono una casella di posta istituzionale devono essere nominate dal responsabile dell'area della struttura afferente;

5. Eventuali copie di sicurezza del contenuto delle cassette email assegnate sono a carico dell'utente assegnatario/proprietario.

Credenziali per l'accesso a Microsoft 365 e alla casella di posta elettronica

1. L'accesso alla casella di posta elettronica del CNDCEC avviene mediante le credenziali di Microsoft 365;

2. le credenziali di accesso alla casella di posta elettronica vengono consegnate dai Sistemi Informativi, all'assunzione del dipendente/inizio del rapporto di collaborazione (ove autorizzato) e devono essere obbligatoriamente modificate la primo accesso;

3. le credenziali vengono immediatamente revocate/annullate dai Sistemi Informativi, alla cessazione del rapporto di dipendenza/collaborazione con Il CNDCEC tramite comunicazione da parte del responsabile di area o dall'ufficio del personale);

4. le credenziali di accesso attribuite dai Sistemi Informativi sono modificabili in totale autonoma dall'utente;

5. l'utente è tenuto a rispettare le policy per la creazione di password sicure e per la sostituzione programmata stabilita dall'amministratore di sistema;

6. l'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla casella di posta elettronica consapevole che la cessione delle stesse consente ad altri l'accesso ai servizi di posta con possibilità di inviare e ricevere mail a nome dell'utente abilitato;

7. la responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione alla casella di posta elettronica sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti di terzi che del CNDCEC, di fatti e atti illeciti. Quanto sopra vale per le caselle di posta elettronica istituzionali condivise alle quali si accede per tramite del proprio account;

8. qualora l'utente debba allontanarsi dalla propria postazione di lavoro, al fine di prevenire accessi incontrollati da parte di terzi è tenuto ad uscire dalla casella di posta elettronica;

9. è assolutamente proibito l'accesso a caselle di posta dell'Ente diverse da quella/e assegnate;

10. l'utente si impegna a modificare tempestivamente la password d'accesso alla casella di posta qualora tale dato sia stato rubato, smarrito o sia noto a terzi;

11. in caso il dato si sia diffuso in maniera fraudolenta a persone terze (furto, sottrazione illecita, copia non autorizzata, operazioni di pirateria informatica, ecc.) l'utente deve comunicare tempestivamente l'accaduto ai Sistemi Informativi;

12. nel caso l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata al responsabile dell'ufficio;

13. i dati e la corrispondenza intercorsa sono mantenuti riservati e possono essere resi disponibili a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

Utilizzi consentiti della posta elettronica

La casella di posta è uno strumento di lavoro assegnato all'atto dai Sistemi Informativi. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

1. È fatto divieto di inviare/ricevere posta elettronica su caselle diverse da quelle assegnate dal CNDCEC all'utente;

2. non è consentito l'utilizzo della posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate. In particolare è fatto divieto di utilizzare le caselle di posta elettronica del CNDCEC per l'invio di messaggi personali;

3. è fatto divieto di utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;

4. la posta elettronica diretta all'esterno della rete informatica del CNDCEC può essere intercettata da estranei, e dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati";

5. l'utente è tenuto a seguire attentamente le disposizioni date dai Sistemi Informativi riguardanti la protezione da virus e da altri software che possano diffondersi via mail;

6. è vietato l'utilizzo di tecniche di "mail spamming" cioè l'invio massivo di comunicazioni a liste di comunicazioni extra CNDCEC non autorizzate dal responsabile di area e/o di azioni equivalenti;

7. nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer, ma disconnettendolo immediatamente dalla rete internet;

- segnalare l'accaduto ai Sistemi Informativi.

8. Il CNDCEC mette a disposizione degli utenti sistemi di avviso automatico che in caso di assenza prolungata permettono d'informare i mittenti dell'assenza e forniscono coordinate e riferimenti all'interno del CNDCEC tali da garantire il corretto funzionamento dei servizi. L'attivazione è a cura dell'utente utilizzatore della casella di posta elettronica.

Contenuto dei messaggi

1. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

2. gli utenti devono prestare attenzione nell'invio di messaggi elettronici affinché non siano inserite inconsapevolmente delle informazioni su credenziali utilizzate in altre applicazioni;

3. gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi;

4. è esplicitamente vietato l'invio di messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte;

5. Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti" nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

Altre istruzioni riguardanti la posta elettronica

1. Gli utenti sono invitati ad inviare allegati in formati comuni possibilmente senza funzioni macro. L'incapacità per il destinatario di aprire file con estensioni poco comuni potrebbe comportare la cancellazione del messaggio (scambiato per un allegato dannoso).

2. Gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo devono prestare molta attenzione nella selezione dei destinatari.

3. Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta. Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo può compromettere sensibilmente la stabilità del programma di posta.

4. Gli utenti devono sempre indicare con chiarezza nel campo oggetto, l'argomento del proprio messaggio.

5. E' possibile richiedere una ricevuta di lettura / ricevimento della propria mail. A tale ricevuta va tuttavia assegnata un'importanza relativa.

6. La conferma della ricezione avviene per opera del mail server centrale e non del destinatario ultimo del messaggio. Non sempre il destinatario conferma la lettura di un messaggio o utilizza sistemi di posta elettronica compatibili, pertanto non vi è certezza sullo stato di ricezione del messaggio.

7. Gli utenti sono invitati a porre attenzione a mail provenienti da mittenti sospetti, mail il cui messaggio riporti errori di ortografia o lessicali e/o contenenti allegati inconsueti non accompagnati da alcun messaggio di testo.

8. Gli utenti che sospettano di aver ricevuto mail malevole non debbono mai inoltrarle ad altri.

8. Si raccomanda di prevedere, con la funzione di inserimento automatico della firma in calce all'email, la seguente avvertenza sulla privacy e sulla confidenzialità dei messaggi inviati: *"Questo messaggio è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo e-mail."*

Raccomandazioni sull'utilizzo e la gestione dei dati del CNDCEC su dispositivi personali

- Utilizzare i sistemi operativi per i quali è garantito il supporto
- Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo
- Assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati
- Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura
- Non installare software proveniente da fonti/repository non ufficiali
- Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro
- Non cliccare, e non inoltrare, su link o allegati contenuti in email sospette
- Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette
- Utilizzare dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dal CN).
- Effettuare sempre il log-out dai servizi/portali utilizzati dopo che aver concluso la sessione lavorativa
- Prestare la massima attenzione alla protezione dei dispositivi mobili: abilitare le funzionalità antifurto come l'individuazione della posizione del dispositivo, il blocco e la cancellazione dei dati, il blocco dello schermo e la password, e il Face ID o il Touch ID: abilitare il controllo delle applicazioni per garantire che siano installate solo quelle della white list.