Ufficio Risorse umane, formazione,
transizione al digitale e sistemi informativi

STRALCIO REGOLAMENTO sull'utilizzo delle risorse informatiche e telefoniche del Consiglio Nazionale dell'Economia e del Lavoro

Prefazione

Estensori del Documento:

- Ufficio III - Gestione delle Risorse Umane e la formazione; per la transizione digitale e dei sistemi informativi; per la revisione delle procedure, dei modelli di lavoro e per la realizzazione del fascicolo informatico
- Data Protection Officer

Informazioni Privacy

Nel presente documento vengono illustrate procedure interne al CNEL, dove possono essere riportate informazioni di natura sensibile. In particolare, nomi degli utenti, username, numeri telefonici ed indirizzi mail.

Data	Versione	Autore	Note
25-08-2022	0.1	Ufficio III e DPO	Prima Stesura

SOMMARIO

Art. 6 - Utilizzo della infrastruttura di rete

6.1 Per l'accesso agli strumenti informatici dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto previsto dall'art. 5.

6.2 È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisione di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per Ufficio o per diversi criteri o per obiettivi specifici di lavoro. Gli strumenti Informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto, non è consentito il salvataggio sui server dell'Ente, ovvero sugli strumenti informatici, di documenti non inerenti all'attività lavorativa. Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli strumenti informatici viene rimosso secondo le regole previste dal presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

6.4 Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell'Amministratore di Sistema e non sono oggetto di backup periodici. A titolo meramente esemplificativo e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o nella disponibilità personale come hard disk portatili o NAS ad uso esclusivo. Pertanto, la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

6.5 A meno di espressa autorizzazione e per ragioni di servizio da parte del

Dirigente dell'Ufficio di appartenenza, non è consentito trasferire documenti elettronici dai sistemi informativi e strumenti dell'Ente a device esterni (hard disk, chiavi USB, CD, DVD e altri supporti).

6.6 Senza il consenso dell'Amministratore di Sistema è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo strumento informatico in dotazione) su repository esterne (quali ad esempio Dropbox, Google Drive, OneDrive, WeTransfer, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi. In caso di necessità l'Ente dovrà mettere a disposizione modalità in linea con le presenti direttive.

6.7 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6.8 All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "WiFi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete WiFi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente ed in occasione di convegni a relatori e partecipanti che necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione WiFi sarà effettuata dall'Amministratore di Sistema.

6.9 L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la

sicurezza informatica.

Art. 11 - Assistenza agli utenti

11.1 L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

11.2 Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

11.3 L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

Art. 12 - Controllo sugli strumenti informatici

12.1 L'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il Titolare del trattamento, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2, L. 300/1970), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinino un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dei principi di cui all'art. 3 del presente regolamento.

12.2 L'uso degli strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.).

Gli interventi di controllo, di seguito descritti, possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti in dotazione:

a) ***Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, ecc.)*** - Qualora risulti necessario l'accesso agli Strumenti

informatici ed alle informazioni ivi contenute, il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo:

- avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento;
- successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo a rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;
- qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali sopra descritti, il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.

b) ***Controlli per esigenze produttive e di organizzazione.***

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile

con lo Strumento oggetto di controllo):

- redazione di un atto da parte del Dirigente dell'Ufficio competente che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
- incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
- redazione di un verbale che riassuma i passaggi precedenti.

In ogni caso, l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal GDPR.

Art. 14 - Partecipazione a Social Media

14.1 L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

14.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione del Titolare.

14.4 L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci

registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile al trattamento dei dati personali.

14.5 Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.


REPUBBLICA ITALIANA
CNEL
CONSIGLIO NAZIONALE ECONOMIA E LAVORO