Sistemi Informativi

Regolamento interno per utilizzo dei Sistemi e strumenti Informatici

ENIT S.p.A.

	Elaborato	Verificato	Approvato
Direzione/Funzione	Sistemi Informativi	Direttore Generale	
Responsabile	Sabrina De Paolis	Elena Nembrini	
Data	Roma 16.10.2024	Roma 26.02.2025	

Scopo e Ambito

Il presente Regolamento ha lo scopo di definire le norme e le linee guida per l'uso corretto dei sistemi informatici aziendali, al fine di garantire la sicurezza delle informazioni,e tutelare i beni aziendali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre la Società a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare la Società ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.
A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento UE n. 2016/679, al d.lgs. n. 196/2003 come modificato dal d.lgs. n. 101/2018, alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provv. 1 marzo 2007)
Il presente Regolamento si applica ad ogni *Utente* e *Destinatario* assegnatario ovvero utilizzatore di beni, risorse informatiche e più in generale di *Sistemi Informatici* aziendali.

Definizioni

Sistemi Informatici: Tutti i personal computer fissi o mobili, server, reti, software, dispositivi mobili telefoni, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc) e altre tecnologie informatiche di proprietà o gestiti dall'azienda.

Utenti: personale dipendente, personale comandato o distaccato, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e tutte le persone autorizzate ad accedere e utilizzare i sistemi informatici aziendali.

Destinatari

Il presente Regolamento si applica sia ai dipendenti Enit S.p.A. della Sede Centrale che a tutti i dipendenti delle Sedi Estere compresi gli Uffici di Rappresentanza, per gli aspetti compatibili, a tutti coloro che, in virtù di altre formule contrattuali, si trovino ad agire avendo la disponibilità regolamentata di accesso ai sistemi informativi.

Titolarità degli strumenti informatici

I beni e le risorse informatiche, i servizi ICT e le reti informative e tutti i *Sistemi Informatici* costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà della Società. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente e Destinatario in base al rapporto in essere

(ovvero per scopi professionali afferenti l'attività svolta per la Società), e comunque per l'esclusivo perseguimento degli obiettivi aziendali. A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni, delle risorse informatiche e più in generale dei *Sistemi informatici* di proprietà della Società, sarà dallo stesso considerato come avente natura aziendale e non riservata.

Responsabilità personale

Gli *Utenti* e i *Destinatari* sono personalmente responsabili dell'utilizzo dei *Sistemi Informatici* affidatigli dalla Società nonché dei relativi dati trattati per finalità aziendali. A tal fine gli stessi, nel rispetto dei principi di diligenza, sono tenuti a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali. Ogni Utente e Destinatario, pertanto, è tenuto, in relazioni al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno. Sono vietati comportamenti che possano creare un danno, anche di immagine, all' Ente.

Controlli

La Società, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente. Ciononostante, non si esclude che, per ragioni organizzative ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tali casi, infatti, sarà onere della Società sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali ovvero, in assenza di queste, con la commissione interna. In difetto di accordo, su istanza della Società, provvederà l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati. La Società, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della "gradualità".

Secondo questo principio:
- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative.
- Nel caso in cui si dovessero riscontrare violazioni del presente Regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.

- In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati

In ogni caso la Società non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso; -
- la memorizzazione sistematica delle pagine internet visualizzate, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi dei dispositivi per l'accesso alla rete internet;

Accesso e Autenticazione

Le credenziali di accesso vengono assegnate dal Responsabile dei Sistemi Informativi, al momento dell'assunzione e consistono in un codice per l'identificazione dell'utente (user-id o username) associato ad una parola chiave riservata (password).

Gli utenti sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione e devono utilizzarle e gestirle attenendosi alle seguenti istruzioni:

- la parola chiave, assegnata è composta da un minimo di otto caratteri o comunque dal massimo di caratteri consentito dal sistema; deve essere puntualmente sostituita al primo utilizzo e laddove non prevista la sostituzione automatica governata dal server, deve essere modificata ogni 30 giorni;
- gli utenti devono utilizzare credenziali univoche (username e password) per accedere ai sistemi informatici;
- le password devono essere complesse e cambiate regolarmente, seguendo le linee guida specificate dall'azienda;
- gli account di accesso non devono essere condivisi tra più utenti;
- la password non deve contenere riferimenti agevolmente riconducibili all'utente e dovrebbe essere generata preferibilmente senza un significato compiuto;
- l'utente, nello scegliere la propria password, deve utilizzare anche caratteri speciali, numeri, lettere maiuscole e minuscole. L'utente non deve scegliere come password parole presenti in un dizionario, sia della lingua italiana che di lingue straniere, né utilizzare parole ottenute come combinazione di tasti vicini sulla tastiera o sequenze di caratteri (ad esempio querty, asdfgh, 123321, aabbcc, ecc.);
- la parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- la parola chiave non deve essere scritta su nessun tipo di supporto (cartaceo, elettronico);
- l'utente è responsabile di ogni utilizzo indebito o non consentito delle credenziali di autenticazione di cui sia titolare;

- nel caso in cui altri utenti debbano poter accedere ai dati protetti dalle credenziali di un utente assente, è necessario richiedere l'autorizzazione all'Amministratore di Sistema (Responsabile dei Sistemi Informativi) che provvederà a resettare la parola chiave dell'utente assente il quale, al suo ritorno, dovrà procedere nuovamente al cambio della stessa;
- le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti;
- nel caso l'utente abbia il sospetto di una perdita di qualità delle proprie credenziali (ad esempio perchè crede che queste siano conosciute da altri) è tenuto immediatamente a darne notizia all'Amministratore del Sistema e contestualmente procedere al cambio della parola chiave;

nel caso l'incaricato dimentichi la propria password, dovrà chiedere formalmente all'amministratore del Sistema l'assegnazione di una nuova parola chiave da gestire come indicato al precedente punto.

Salvataggio dei dati e Backup

Tutto il personale è tenuto a salvare i dati utili per lo svolgimento dell'attività lavorativa sulla piattaforma di collaborazione fornita da Enit S.p.A., sviluppata da Microsoft che consente di condividere e archiviare documenti e informazioni (SharePoint, OneDrive, ecc.); in modo tale che i documenti possano essere accessibili da qualsiasi luogo e dispositivo. I dati contenuti nel PC aziendale in dotazione al dipendente ed utilizzati per lo svolgimento dell'attività lavorativa appartengono al patrimonio aziendale.

Di conseguenza, averne l'accesso, non si traduce nel poter disporre dei relativi dati arbitrariamente poiché le informazioni che in esso sono immagazzinate devono pur sempre essere utilizzate per fini lavorativi. Pertanto, il dipendente che cancelli, manipoli o trasferisca all'esterno tali dati, attua una condotta disciplinarmente rilevante, commettendo un illecito sia civile che penale oltre ad essere tenuto al risarcimento dei danni.

E' da considerare il **reato di danneggiamento** per il dipendente che, avendo la disponibilità materiale del PC aziendale, al momento delle dimissioni formatta il PC, cancellando tutti i dati in suo possesso, anche se da lui stesso creati.

I backup dei dati vengono eseguiti automaticamente.

Utilizzo Consentito

I sistemi informatici devono essere utilizzati esclusivamente per scopi lavorativi e attività autorizzate dall'azienda.
È vietato l'uso dei sistemi informatici per scopi personali, giochi, attività illegali o non etiche.

Non è consentito modificare le configurazioni relative all'accesso alla rete (ad esempio indirizzo IP); installare modem per l'accesso da/all'esterno; copiare su dispositivi esterni personali dati la cui titolarità è di Enit S.p.A., installare autonomamente programmi o applicativi.
L'utilizzo dei telefoni di proprietà dell'Enit S.p.A. è consentito solo allo svolgimento delle attività previste per il ruolo ricoperto.
L'utilizzo delle stampanti e dei materiali di consumo (carta, inchiostro, toner chiavi USB, ecc.) è riservato esclusivamente alla preparazione di materiale inerente all'attività istituzionale dell'Enit S.p.A.

Protezione dei Dati

Gli utenti devono proteggere i dati sensibili e riservati dell'Azienda e dei clienti, evitando la divulgazione non autorizzata.
È obbligatorio l'uso di strumenti di crittografia per la trasmissione di dati sensibili via e-mail o altri mezzi digitali.

Sicurezza Informatica

È vietato installare software non autorizzato sui dispositivi aziendali.
Gli utenti devono segnalare immediatamente qualsiasi incidente di sicurezza o sospetto di violazione informatica.
I dispositivi aziendali devono essere protetti da antivirus aggiornati e firewall.
Enit S.p.A. è dotata di un sistema centralizzato di protezione antivirus che si aggiorna con cadenza giornaliera in automatico, sia sui server che sulle postazioni di lavoro, ogni volta che si accende il dispositivo all'interno della rete aziendale.
È assolutamente vietato sospendere, cancellare, non aggiornare o alterare il sistema antivirus anche se il suo funzionamento possa comportare un calo nelle prestazioni delle postazioni di lavoro; ogni danno conseguente alla manomissione de sistema sarà addebitato al manomissore.

Utilizzo di Internet ed E-mail

L'accesso a Internet deve essere utilizzato in modo responsabile e solo per attività legate al lavoro.
È vietato accedere a siti web inappropriati, illegali o non sicuri.
Non è consentito utilizzare la navigazione internet per usi non istituzionali. In particolare, non sono permesse le seguenti attività se non preventivamente autorizzate:

- scaricamento (download) di qualunque genere di file o programmi salvo non sia indispensabile per svolgere attività lavorativa a cui il dipendente è preposto;
- caricamento (upload) di file di qualunque genere presso siti esterni alla rete.

Le e-mail aziendali devono essere utilizzate solo per comunicazioni professionali. Gli utenti devono essere cauti nell'aprire allegati o link provenienti da fonti non affidabili.
Ad ogni utente viene assegnato un indirizzo di posta elettronica istituzionale personale.
Agli utenti potrà essere assegnato un indirizzo di posta funzionale condiviso con altri utenti.

Non è consentito aprire messaggi, né manualmente, né in forma automatica, con allegati di cui non si conosce l'origine in quanto possono contenere virus in grado di danneggiare e/o cancellare i dati sulle postazioni di lavoro.

Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun *Utente* e *Destinatario*, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.
In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), la Società, perdurando l'assenza oltre un determinato limite temporale pari a _10_ giorni, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento (risposta automatica o reindirizzamento), avvertendo l'assente.
Nel caso, invece, la Società necessiti conoscere il contenuto dei messaggi di posta elettronica dell'Utente e del Destinatario resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:
• la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato (per iscritto) dall'Utente assente;
• di tale attività sarà redatto apposito verbale e informato l'Utente interessato alla prima occasione utile.

Cessazione dell'indirizzo di posta elettronica aziendale

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; i terzi verranno informati con meccanismi automatizzati della disattivazione dell'account e saranno loro comunicati indirizzi alternativi a cui rivolgersi; entro 3 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ente si riserva il diritto di effettuare un back up e conservare i messaggi di posta elettronica che riterrà rilevanti.

Gestione delle Risorse

Gli utenti devono utilizzare le risorse informatiche aziendali in modo efficiente e senza sprechi.
È vietato l'uso eccessivo o non necessario di stampanti, larghezza di banda di rete e altre risorse informatiche.

Privacy e Monitoraggio

L'azienda si riserva il diritto di monitorare l'uso dei sistemi informatici per garantire la conformità con questo Regolamento e altre politiche aziendali.
Qualsiasi attività di monitoraggio sarà effettuata in conformità con le leggi sulla privacy applicabili.

Violazioni e Sanzioni

Qualsiasi violazione di questo Regolamento sarà soggetta a sanzioni disciplinari, come previsto dalla normativa di riferimento, regolamenti e codici aziendali.
Le violazioni gravi possono essere segnalate alle autorità competenti.
Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo Regolamento, la Società si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

Riferimenti:

- Regolamento Generale sulla Protezione dei Dati (GDPR);
- Modello di Organizzazione, Gestione e Controllo D.lgs. 231/2001;
- NIS2 16.01.2023 (La direttiva NIS2 fornisce una normativa a livello dell'UE sulla cybersicurezza).

Modifiche al Regolamento

Questo Regolamento potrà essere aggiornato in ragione di cambiamenti ed evoluzioni organizzative aziendali e normative in materia e qualora ritenuto opportuno.
L'aggiornamento al Regolamento dovrà essere sottoposto al CDA per approvazione.
Gli utenti saranno informati di qualsiasi modifica significativa.

Accettazione del Regolamento

Il presente Regolamento è reso pubblico sul sito web istituzionale della Società nella sezione Amministrazione trasparente.