AGENZIA NAZIONALE PER LE
NUOVE TECNOLOGIE, L'ENERGIA E LO
SVILUPPO ECONOMICO SOSTENIBILE

# DISCIPLINARE
## SULL'USO DEI DISPOSITIVI INFORMATICI E DELLA RETE DATI

*Aprile 2024*

# INDICE

*INDICE* ..... *2*
*PREMESSA* ..... *3*
*CAPITOLO 1 PRINCIPI GENERALI* ..... *4*
*CAPITOLO 2 USO DEGLI STRUMENTI INFORMATICI* ..... *9*
*CAPITOLO 3 CESSAZIONE DEL RAPPORTO DI LAVORO* ..... *18*
*CAPITOLO 4 INTERVENTI DI ASSISTENZA E MANUTENZIONE* ..... *19*
*CAPITOLO 5 VERIFICHE, RESPONSABILITA' E SANZIONI* ..... *19*
*CAPITOLO 6 NORME FINALI* ..... *20*
*ALLEGATO 1 - NORMATIVA DI RIFERIMENTO NAZIONALE E INTERNA* ..... *21*

# PREMESSA

Il Disciplinare sull'uso dei dispositivi informatici e della rete dati (nel seguito *Disciplinare ICT*) è redatto in conformità ai riferimenti normativi, richiamati nell'ALLEGATO 1 - NORMATIVA DI RIFERIMENTO NAZIONALE E INTERNA, dal Gruppo di Lavoro appositamente predisposto e periodicamente aggiornato in coordinamento tra le strutture di ENEA con competenza sulle materie trattate.

La diffusione sempre più capillare delle tecnologie informatiche ed il libero accesso alla rete Internet, tramite i dispositivi elettronici di proprietà o comunque nella disponibilità dell'ENEA, espone l'ENEA, incluso il suo patrimonio materiale e immateriale, il personale in organico (dipendenti e collaboratori), ed i soggetti terzi presenti, a rischi derivanti dall'acquisizione abusiva, perdita, distruzione, indisponibilità, modifica, corruzione e diffusione incontrollata di dati personali e non. Ciò, oltre a determinare un possibile danno all'immagine dell'ENEA, può comportare responsabilità giuridiche di varia natura dalle quali possono scaturire obblighi risarcitori e sanzioni di natura amministrativa, contabile e penale.

I rischi concreti che ne possono derivare sono, sostanzialmente, riferibili:

- ai diritti, alle libertà e alla sicurezza delle persone;
- alla sicurezza ed integrità del patrimonio materiale dell'ENEA (beni patrimoniali, infrastrutture fisiche, ecc.);
- alla protezione del patrimonio immateriale dell'ENEA (know-how, processi, informazioni e misure di sicurezza interne, ecc.).

Sui predetti sistemi informatici è altresì vietata la trattazione di informazioni classificate o classificabili ai sensi della normativa che disciplina il settore della sicurezza nazionale (Legge 124/2007 e s.m.i.).

È indispensabile che le regole suddette siano applicate in maniera efficace, proporzionata ai rischi ed al possibile impatto, nonché siano contestualizzate all'attività da svolgere senza pregiudicarne l'agilità operativa e la funzionalità.

# CAPITOLO 1 PRINCIPI GENERALI

**ART.1.** *Oggetto e finalità*

A) Oggetto

Il *Disciplinare ICT* intende:

I. **Disciplinare**:

- il corretto utilizzo delle risorse informatiche, fisse e mobili;
- le procedure ed i sistemi di analisi, di controllo e prevenzione necessari ad assicurare il buon funzionamento della rete ed il perseguimento dei fini statutari dell'ENEA, nel rispetto delle norme giuridiche in vigore e delle altre norme interne adottate dall'ENEA;
- i mezzi ed i modi con cui i lavoratori sono tenuti a trattare i dati registrati o comunque acquisiti su supporti informatici, inclusi quelli personali e quelli soggetti a speciali tutele.

II. **Presentare**:

- ai lavoratori un quadro di riferimento strutturato ed omogeneo, al fine di adottare i corretti comportamenti sui mezzi ed i modi con i quali ENEA, in quanto Titolare o Responsabile del trattamento, tratta i dati, e sulle norme e cautele che i lavoratori autorizzati ad accedere ai dati devono adottare, inclusi quelli personali e quelli soggetti a speciali tutele.

B) Finalità

Il *Disciplinare ICT* intende:

I. **Garantire**:

- sicurezza, resilienza e funzionalità dei sistemi e delle infrastrutture ICT;
- prevenzione e supporto per la pronta risoluzione di eventuali problemi tecnici;
- la tutela dei diritti degli interessi e dell'immagine dell'ENEA;
- la conformità alle norme in materia di protezione dei dati, inclusi quelli personali e quelli soggetti a speciali tutele;
- la corretta conduzione del rapporto di lavoro.

II. **Tutelare**:

- l'organizzazione delle attività dell'ENEA e la loro agibilità;
- il rispetto di obblighi di legge;
- l'integrità dei beni e delle infrastrutture dell'ENEA;
- la sicurezza dei dati, inclusi quelli personali e quelli soggetti a speciali tutele, e la loro fruibilità nei contesti autorizzati alla specifica trattazione.

**ART.2.** *Ambito di applicazione soggettivo e oggettivo*

Il *Disciplinare ICT* si applica ai lavoratori ENEA (V. definizione ART. 3 lett. N) e ne disciplina il comportamento in relazione alla gestione e all'utilizzo degli strumenti informatici; tutti i lavoratori sono formati, informati e tenuti all'osservanza del suddetto Disciplinare.

**ART.3.** *Definizioni*

Ai fini del *Disciplinare ICT* si intende per:

*A)* ***"Amministratore di Sistema"*** *o* ***AdS****: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione dati, compresi i sistemi di gestione delle banche dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui gli siano attribuiti dal Designato al coordinamento (cfr. Circolare n. 22/2020/PRES del 7/7/2020 "Adozione del funzionigramma privacy") i privilegi necessari e sufficienti per intervenire su dati o informazioni, inclusi quelli personali e quelli soggetti a speciali tutele. Gli AdS operano in regime speciale, in ragione dei privilegi informatici detenuti, per cui sono concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevati livelli di criticità rispetto alla protezione dei dati.*

*Non sono qualificabili come AdS:*

- *i lavoratori cui vengono concessi, in via eccezionale, i privilegi di amministratore di dispositivi informatici per uso personale;*
- *coloro che non sono designati come AdS dal Designato al coordinamento.*

*B)* ***"Collaboratori"****: chiunque esegua una prestazione a favore dell'ENEA indipendentemente dalla qualificazione del rapporto giuridico sottostante.*

*C)* ***"Dati Personali"****: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), secondo la definizione di cui all'art. 4 GDPR, ai sensi dei principi vigenti in materia di protezione dei dati.*

*D)* ***"Dati di categoria particolare"****: dati personali di cui all'art. 9 GDPR (che rivelino l'origine raziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici e biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona).*

*E)* ***"Informazioni classificate"****: informazione a cui è stata associata una classifica di segretezza con atto amministrativo deciso dall'originatore stesso dell'atto, sulla base della disciplina recata dalla Legge 124/2007 e ss.mm.ii.; in tal senso le dizioni di "Riservato", "Riservatissimo", "Segreto" e "Segretissimo", e "Confidenziale" nel contesto internazionale, devono essere utilizzate esclusivamente in tale ambito.*

*F)* ***"Dipendenti"****: personale che esegue una prestazione lavorativa, manuale o intellettuale, in favore dell'ENEA, dietro pagamento di un compenso e sotto le direttive del datore di lavoro per quanto*

*riguarda luogo di lavoro, orario e mansioni svolte; rientrano in questa categoria: i/le dipendenti a Tempo Determinato, i/le dipendenti a Tempo Indeterminato, i/le dipendenti in quiescenza con contratti di collaborazione con ENEA.*

*G)* ***"Dispositivi informatici"*** *(vedi Strumenti informatici).*

*H)* ***"DPO"*** *(Data Protection Officer) o "RPD" (Responsabile della Protezione dei Dati personali): soggetto designato dal Titolare del trattamento (cfr. successiva lettera I) a svolgere le funzioni di supporto, controllo e prassi formative e informative sulle disposizioni previste dal GDPR, in affiancamento il titolare e/o al responsabile del trattamento (cfr. relative definizioni).*

*I)* ***"Titolare del trattamento"****: la persona giuridica ENEA, che singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.*

*J)* ***"FAS"*** *o* ***"Funzionario alla Sicurezza"****: soggetto delegato dall'organo di vertice dell'ENEA a svolgere le funzioni previste dal DPCM 5/2015.*

*K)* ***"Internet"****: network di computer, una serie di reti (private, pubbliche, aziendali, universitarie, commerciali) connesse tra loro fino a raggiungere una dimensione di accesso globale.*

*L)* ***"Infrastruttura informatica"****: insieme dei dispositivi hardware e software che compongono, collegano e regolano il sistema informatico dell'ENEA.*

*M)* ***"Infrastruttura di rete"****: insieme di dispositivi hardware e software, compresi i canali di comunicazione, che permettono la comunicazione informatica tra due o più utenti, consentendo di trasferire risorse, informazioni e dati.*

*N)* ***"Lavoratore ENEA"*** *o* ***"Lavoratore":*** *dipendente ed ogni altro soggetto che, indipendentemente dall'inquadramento lavorativo e se del caso senza vincolo di subordinazione, tratti dati e informazioni appartenenti al patrimonio informativo e/o utilizzi la rete dati ENEA mediante l'uso di strumenti informatici messi a disposizione da ENEA o personali.*

*O)* ***"Lavoro agile"*** *(LAG): Per "lavoro agile" o "smart working" si intende una nuova modalità flessibile di esecuzione rapporto di lavoro subordinato consistente in una prestazione di lavoro svolta in parte all'interno della sede di lavoro ed in parte all'esterno, entro i soli limiti massimi dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge o contrattazione collettiva, senza la previsione di una postazione fissa durante i periodi svolti al di fuori dei locali dell'Agenzia e con l'utilizzo di strumenti tecnologici.*

*P)* ***"Profilo utente"*** *o* ***"profilo di abilitazione"****: concerne il perimetro delle risorse di rete e di connettività a cui le credenziali attribuite all'utente consentono di accedere; i profili vengono assegnati dalla Divisione TERIN-ICT e biunivocamente connessi al nominativo utente su richiesta del Servizio del Personale e del Responsabile di struttura in funzione dell'attività svolta dall'utente stesso.*

*Q) **"Postazione di Lavoro":** ogni Dispositivo informatico concesso da ENEA al Lavoratore in uso personale.*

*R) **"Responsabile dei Sistemi Informatici"**: soggetto incaricato di progettare e gestire le attività dirette a garantire la sicurezza e il funzionamento dell'infrastruttura informatica secondo quanto meglio indicato nella declaratoria del ruolo istituzionale del Responsabile della Divisione TERIN-ICT, in coordinamento strategico con il RTD (cfr. definizione RTD).*

*S) **"RPD"** (Responsabile della Protezione dei Dati personali): cfr. definizione di DPO.*

*T) **"RTD"** (Responsabile della Transizione Digitale): figura dirigenziale prevista dal Codice dell'Amministrazione Digitale, D.lgs. 82/2005 (CAD), e disciplinata dall'art.17 del CAD e ss.mm.ii.*

*U) **"Responsabile del Servizio/Applicazione"**: soggetto che supervisiona le attività connesse all'erogazione di un servizio ICT, sia esso rivolto ai dipendenti che ad utenti esterni.*

*V) **"Responsabile del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; l'ENEA può essere sia Titolare (e contitolare) che Responsabile del trattamento dei dati personali.*

*W) **"Designato al Coordinamento"**: ai sensi della Circolare n. 22/2020/PRES "Adozione del funzionigramma privacy", si tratta dei Responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono:*

*- per le Direzioni e le Unità/Istituti: i/le Dirigenti delle Direzioni per le attività di propria competenza ed i/le Responsabili delle altre Unità/Istituti;*

*- per i Dipartimenti: i/le Direttori/Direttrici dei Dipartimenti.*

*X) **"Strumenti Informatici"** o **"Dispositivi informatici":** strumenti anche solo potenzialmente idonei ad accedere ad Internet ed ai suoi servizi, detti anche "host" o "macchine client" o "client". Rientrano in questa categoria: PC, notebook, tablet, smartphone, cuffie audio, microfoni, tastiere, mouse, monitor, macchine fotografiche, telecamere, fax, stampanti, fotocopiatrici, IoT, compresi i programmi software, le applicazioni e gli altri strumenti idonei ad accedere ad Internet.*

*Y) **"Supporti removibili"**: si intendono tutti i supporti di memorizzazione di dati rimovibili (e.g. CD, DVD, pen drive, schede di memoria, hard disk esterni, etc.).*

*Z) **"Divisione TERIN-ICT"**: Unità dell'ENEA costituita da personale che agisce sotto il controllo e la responsabilità del Responsabile dei Sistemi Informatici. Lo scopo della Divisione TERIN-ICT è, tra le altre cose, di compiere tutte le attività operative atte alla modellizzazione, alla strutturazione nonché garantire il buon funzionamento generale dell'infrastruttura informatica ENEA (sicurezza informatica, backup, rete, server, progettazione informatica ecc.); la suddetta Divisione dedica proprie risorse allo svolgimento di tali attività ed a tal fine emana, in coordinamento strategico con il RTD (cfr. definizione RTD) , documenti di indirizzo sul corretto impiego di hardware e software.*

*AA) **"SOC**" - Security Operation Center: gruppo di esperti ICT provenienti da diverse Unità di struttura ENEA. Rappresenta il centro di coordinamento di tutti i processi di emergenza provocati da una eventuale minaccia, al fine di ridurne gli impatti in caso di minaccia accertata. Il SOC si occupa anche di servizi di difesa preventiva e di protezione.*

*BB) **"Telelavoro"** (o TLV): con telelavoro si intende una modalità di prestazione di lavoro svolta da un dipendente in qualsiasi luogo compatibile con i progetti di telelavoro di cui allo specifico Regolamento ENEA (cfr. allegato 1 del presente documento "Normativa Interna Enea"), esterno alla sede ufficiale di lavoro alla quale risulta assegnato, dove la prestazione a distanza sia tecnicamente possibile e comunque sul territorio italiano.*

*CC) **"WEB":** sistema di accesso a documenti in formato ipertestuale, posti in relazione per mezzo di link e accessibili mediante Intranet e Internet.*

*DD) **"PEC"**: la posta elettronica certificata o PEC è un tipo particolare di posta elettronica che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una tradizionale raccomandata con avviso di ricevimento, garantendo così la prova dell'invio e della consegna.*

*EE) "**Firma Digitale**": con firma digitale si intende un metodo di autenticazione digitale (regolamentato dall'art.24 del CAD) che, attestando l'autenticità del documento (o dell'insieme di documenti a cui è apposta) e identificando univocamente l'autore, consente di scambiare in rete documenti con piena validità legale.*

FF) ***"Log"**:* registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori.

## CAPITOLO 2 USO DEGLI STRUMENTI INFORMATICI

**ART.4.** *Strumenti e dispositivi: criteri generali*

A) L'utilizzo di tali strumenti da parte dei *Lavoratori* deve essere finalizzato allo svolgimento delle mansioni proprie attribuite e al raggiungimento degli obiettivi/scopi dell'ENEA. L'utilizzo non inerente all'attività lavorativa può, infatti, contribuire ad innescare disservizi, maggiori costi di manutenzione e recare minacce alla sicurezza del patrimonio materiale e immateriale dell'ENEA, nonché arrecare pregiudizio al corretto trattamento ed all'adeguata protezione dei dati.

B) Nell'utilizzare gli *Strumenti informatici* il dipendente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del Codice civile e più in generale del relativo titolo 3°, nonché dell'articolo 11, comma 3 del decreto del Presidente della Repubblica 16 aprile 2013, n. 62 "regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del decreto legislativo 30 marzo 2001, n. 165", dell'art. 11-bis, rubricato "Utilizzo delle tecnologie informatiche" e dell'art. 11-ter, rubricato "Utilizzo dei mezzi di informazione e dei social media", introdotti dal D.P.R. 13 giugno 2023, n. 81 in modifica del D.P.R. 16 aprile 2013, n. 62 cit.; inoltre, si richiama quanto previsto dal CCNL Istruzione e Ricerca 2019-2021, Titolo V, Responsabilità disciplinare che, all'art. 23, definisce quali siano i comportamenti del dipendente nello svolgimento del rapporto di lavoro con l'Amministrazione di appartenenza.

C) Conseguentemente, comportamenti difformi da quanto disposto nel presente *Disciplinare ICT,* nei suoi allegati e nei suddetti disposti normativi e codici di comportamento, possono essere oggetto di valutazione da un punto di vista disciplinare e/o determinare una responsabilità giuridica diretta dell'autore.

D) Tutti i lavoratori sono formati e informati in merito ai rischi e alle problematiche relative alla sicurezza in materia di trattamento dei dati sull'utilizzo degli *Strumenti informatici*.

E) Non sono installati o configurati sugli *Strumenti informatici* in uso ai lavoratori apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

F) Tutti i supporti rimovibili devono essere trattati con particolare cautela, diligenza e riservatezza e non devono essere lasciati incustoditi o facilmente accessibili, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato da terzi. A tal fine il datore di lavoro fornisce in maniera esclusiva i supporti per le attività dell'ENEA, cercando di limitare l'utilizzo di supporti rimovibili provenienti da fonti sconosciute. L'utilizzo di supporti rimovibili, rimane in ogni caso sotto la responsabilità dell'utilizzatore, che è tenuto a rivolgersi al servizio di assistenza ICT per le opportune configurazioni di sicurezza e/o crittografia del supporto.

G) I *log* relativi all'utilizzo di applicazioni, reperibili nella memoria del *Dispositivo informatico*, ovvero sui server o sui router, nonché i file ad essi associati, sono registrati e possono essere oggetto

di analisi da parte del Datore di lavoro nei limiti e con le garanzie precisate al successivo art. 13.

H) Le indicazioni del presente *Disciplinare ICT* si applicano anche al collegamento alla rete aziendale da postazioni esterne all'ufficio (ad esempio collegamento in Smart working o in Telelavoro). Sono fatte salve diverse disposizioni formali eventualmente emanate dall'ENEA per regolamentare specifiche necessità sopraggiunte.

**ART.5.** *Postazione di lavoro*

In funzione del ruolo e delle mansioni o compiti che deve svolgere, considerate le esigenze organizzative ed operative, di norma il *Lavoratore* è dotato di uno o più dispositivi informatici per lo svolgimento di attività inerenti o comunque connesse agli incarichi lavorativi. L'ENEA intende assicurare il corretto impiego degli *Strumenti ICT* e della telefonia da parte dei *Lavoratori*, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa.

Ciò avviene nell'ottica di garantire la sicurezza, la disponibilità e l'integrità dei sistemi e di prevenire sprechi. Esiste, quindi, in capo ai lavoratori l'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa, e questo anche nel regolare utilizzo delle risorse ENEA.

A) L'indebito utilizzo della connessione Intranet, Internet e della posta elettronica da parte di un dipendente configura profili di responsabilità a carico del medesimo. A seguito di ripetute e significative anomalie (ad esempio presenza di virus o attacchi informatici), l'ENEA è autorizzata a svolgere verifiche anche *ex post* sulle singole postazioni coinvolte nelle anomalie (v. Cap. 5); in particolare, come stabilisce il Titolo V "Responsabilità disciplinare", art. 23,comma 3 lettera a) del CCNL vigente, il dipendente è tenuto a collaborare con diligenza osservando le disposizioni impartite dall'amministrazione anche in relazione alle norme vigenti in materia di sicurezza e di ambiente di lavoro. In tal senso vanno lette le raccomandazioni di seguito riportate.
B) Le *Postazioni di Lavoro*, normalmente, sono connesse alla rete interna dell'ENEA con lo scopo di usufruire dei servizi, accedere alle applicazioni software gestite centralmente, condividere informazioni, fruire i contenuti Intranet ed Internet per gli scopi lavorativi.
C) L'archiviazione di informazioni nella postazione deve essere finalizzata allo svolgimento della propria attività lavorativa.
D) Il salvataggio (backup) dei dati necessari all'attività lavorativa per le postazioni che non memorizzano i propri dati sul file server centrale è di esclusiva responsabilità del lavoratore.
E) Per tutti i dispositivi informatici è univocamente noto il Profilo Utente a cui il dispositivo è associato.
F) La Divisione TERIN-ICT predispone una configurazione standard basata sul profilo utente di

accesso per il corretto svolgimento delle attività lavorative del personale ENEA. È proibita l'installazione, da parte del lavoratore, di software privo di licenza e/o non inerente all'attività lavorativa, ovvero non espressamente autorizzata dalla Divisione TERIN-ICT e, in caso contrario, ne risponderà personalmente. In caso di dubbi sulle funzionalità di un software il lavoratore potrà richiedere il supporto della Divisione TERIN-ICT, attraverso il portale ticketing dedicato. La richiesta di software aggiuntivi, rispetto alla configurazione standard, va inviata alla Divisione TERIN-ICT attraverso il portale ticketing, per le valutazioni di merito. È altresì proibito modificare la configurazione hardware o software della Postazione di Lavoro assegnata.

G) L'attivazione o la modifica della password di protezione del BIOS del computer o per la cifratura "hardware" del disco è consentita solo dall'AdS a seguito di esplicita autorizzazione della Divisione TERIN-ICT.

H) Non è generalmente consentito utilizzare risorse informatiche e supporti privati per lo svolgimento della propria attività lavorativa (tablet, smartphone, periferiche etc.), salvo casi di necessità, lavoro agile (LAG), telelavoro (TLV) e/o forza maggiore adeguatamente motivati e autorizzati.

I) L'installazione, riproduzione o la duplicazione di programmi, può essere effettuata solo per esigenze connesse alla prestazione lavorativa e in conformità alla vigente normativa in materia di protezione della proprietà intellettuale.

J) Per la duplicazione di documenti contenenti *dati particolari* (v. art. 3 lett. D) su supporti rimovibili o su sistemi di rete non gestiti da ENEA è necessario informare la Divisione TERIN-ICT e il -RPD per le valutazioni di competenza.

K) È rigorosamente vietata l'installazione non autorizzata sulla rete interna ENEA di dispositivi o apparati di rete attivi, ad esempio: Access Point, Router, Printer server, modem, IoT, etc.

L) In caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare denuncia all'autorità competente, è obbligatorio informare tempestivamente la propria Unità di appartenenza, la Divisione TERIN-ICT ed il RPD, comunicando quali dati erano contenuti all'interno della memoria locale del dispositivo per le valutazioni di competenza e le azioni interne ed eventualmente esterne del caso.

M) Al termine delle attività di lavoro deve essere correttamente chiusa la sessione di lavoro ("logout"). In occasione della temporanea sospensione dell'attività lavorativa ed in ogni caso in cui il lavoratore si allontana dalla postazione di lavoro, deve essere attivata la funzione di sospensione o comunque una funzione che renda il dispositivo accessibile solo previo inserimento di una password.

N) Costituisce buona prassi effettuare con cadenza periodica (almeno ogni sei mesi) la pulizia degli

archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati.

O) Non è consentito l'uso di software e sistemi operativi deprecati, per ulteriori informazioni si rimanda all'area Intranet della Divisione TERIN-ICT, dove non sono presenti aggiornamenti di sicurezza che ne assicurino l'affidabilità e possano quindi, con la loro presenza in rete, compromettere la sicurezza della infrastruttura informatica ENEA. Per qualsiasi verifica è necessario rivolgersi al servizio di assistenza ICT.

P) La tutela della gestione locale dei dati presenti sulle postazioni di lavoro personali è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, salvataggi su supporti di rete autorizzati (EneaBox, OneDrive, Share di rete o altri supporti autorizzati).

Q) Nel caso in cui esista la necessità di elaborare banche dati personali in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei Dati Personali informando il DPO.

R) Ai soli fini di prestare assistenza tecnica informatica ordinaria ai lavoratori, l'ENEA utilizza software che permettono all'*AdS* di vedere in tempo reale la sessione di lavoro utente ed eventualmente di intervenire attivamente. L'attivazione di tale funzionalità avviene a valle dell'apertura di un ticket sull'apposito portale ENEA. Il supporto remoto avviene in presenza dello stesso utilizzatore che ha aperto il ticket e su sua esplicita autorizzazione a procedere.

S) L'ENEA può svolgere, attraverso i propri Responsabili di struttura, gli accertamenti necessari e adottare ogni misura a garanzia della sicurezza dei sistemi informatici.

T) Ai fini della sicurezza delle infrastrutture ENEA (quale insieme di hardware, software e relativi supporti trasmissivi), nel momento in cui il SOC identifichi un'attività anomala tale dal compromettere l'integrità della stessa lo stesso SOC agisce senza indugio, tenendo informato il Responsabile del Servizio/Applicazione *e* l'*AdS*, e senza vincoli temporali sulle singole postazioni identificate dalla vulnerabilità individuata.

U) Al Lavoratore è consentito l'utilizzo degli Strumenti informatici forniti dall'ENEA per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

**ART.6.** *Posta elettronica, Pec e firma digitale*

A) Fermo restando il richiamo al precedente obbligo di comportamento, il *Lavoratore* non si avvale di quanto è di proprietà dell'Amministrazione per ragioni che non siano di servizio (Titolo V, articolo 23, comma 3 lettera K) del citato CCNL).

B) La casella di posta, assegnata dall'ENEA al *Lavoratore*, è uno strumento di lavoro e deve essere finalizzato al perseguimento degli scopi lavorativi. Il *Lavoratore* a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa. L'indirizzo fornito è prevalentemente un account e-mail nella forma *nome.cognome@enea.it*.

C) La casella di posta individuale/nominativa viene assegnata, di norma, ai soli Dipendenti ENEA o assimilati (così come descritto all'art. 3 lett. F).

D) La casella di posta elettronica istituzionale, indipendentemente dal carattere nominativo dell'indirizzo, è uno strumento di esclusiva proprietà ENEA, messo a disposizione del dipendente al fine dello svolgimento delle proprie mansioni lavorative, il cui utilizzo non può mai compromettere la sicurezza o la reputazione dell'Amministrazione; la stessa deve essere mantenuta in ordine, cancellando documenti ed e-mail ritenute evidentemente non attendibili al fine di mitigare problematiche di sicurezza.

E) È obbligatorio controllare i contenuti presenti nella e-mail prima della loro apertura. In particolare, si deve prestare molta attenzione, secondo le regole di buona diligenza, nell'operare l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati sconosciuti e potenzialmente pericolosi. In caso di dubbi, non effettuare alcun tipo di interazione sulla mail sospetta e rivolgersi agli *AdS* per assistenza.

F) L'iscrizione a mailing-list o newsletter esterne è consentita esclusivamente per motivi professionali. Prima di iscriversi, occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

G) Non è consentito l'inoltro automatico di e-mail ENEA verso indirizzi privati. In caso di assenza è possibile l'attivazione di un messaggio recante l'indicazione della data di rientro prevista, del nominativo e della e-mail della persona o del Gruppo (lista) a cui rivolgersi.

H) È consentito esclusivamente l'uso di browser o client di posta elettronica (per l'accesso alla casella di posta assegnata da ENEA) che siano stati indicati da ENEA e che comunque rispondano a standard di sicurezza idonei. (cfr. informazioni presenti nell'area Intranet Divisione TERIN-ICT)

I) È vietato l'invio di messaggi di posta elettronica in nome e per conto di un altro utente, se non autorizzato.

J) Il dipendente è responsabile del contenuto dei messaggi inviati; è vietato l'invio di messaggi di posta elettronica all'interno o all'esterno dell'Amministrazione, oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'Amministrazione; è vietato l'inoltro di messaggi altrui, senza il consenso dell'interessato.

K) È richiesto, nei messaggi in uscita, di riportare in calce la firma del soggetto mittente contenente almeno i seguenti dati: nome, cognome ed Unità/Servizio di appartenenza.

L) Poiché la posta elettronica diretta all'esterno della rete informatica ENEA può essere intercettata da estranei, l'invio tramite tale mezzo di documenti di lavoro qualificati a carattere "esclusivo per i/il destinatari/o" è sconsigliato e comunque va valutato con particolare attenzione, eventualmente adottando le opportune cautele quali l'uso di opportune procedure di crittografia con software autorizzati dall'*AdS*.

M) In caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e la tutela del patrimonio ovvero per motivi di sicurezza del sistema informatico, l'ENEA, per il tramite dell'*AdS*, potrà accedere all'account di posta elettronica interessato, prendere visione dei messaggi, acquisirli in memoria, cancellarli, salvare o cancellare file allegati.

N) In caso di cessazione del rapporto lavorativo, la casella di posta individuale verrà disattivata immediatamente. Il dipendente potrà attivare una risposta automatica al mittente, informando che la casella di posta elettronica è stata disattivata. La casella resterà operativa per un anno per la sola ricezione dei messaggi, periodo al termine del quale sarà definitivamente cancellata.

O) ENEA fornisce una casella di posta certificata (PEC) ad alcuni Dipendenti per motivazioni istituzionali. La casella deve essere utilizzata per i soli scopi per cui viene rilasciata e deve essere costantemente controllata in quanto soggetta a documentazione istituzionale dell'EEA. Ritardi nell'acquisizione e conseguenti azioni relativi alla documentazione pervenuta potrebbero comportare danni per l'ENEA. Anche per la PEC valgono le stesse regole e raccomandazioni della posta elettronica ordinaria.

P) ENEA fornisce in esclusiva il servizio di Firma digitale ad alcuni Dipendenti per motivi istituzionali. Il servizio deve essere, pertanto, utilizzato esclusivamente per gli scopi per cui viene rilasciato. Il servizio di firma digitale è strettamente personale e non cedibile a terzi.

**ART.7.** *Uso dei sistemi di comunicazione, collaborazione e canali social*

A) Premesso che i canali di comunicazione social portano sempre alla profilazione dell'individuo, si raccomanda di porre estrema cautela nel divulgare informazioni che, attraverso strumenti di ingegneria sociale (OSINT, Open Source INTelligence), possano essere combinate e correlate mettendo a rischio la sicurezza informatica e danneggiare la proprietà intellettuale delle informazioni stesse dell'ENEA. A tal riguardo, si richiama l'attenzione del dipendente sui contenuti dell'art. 3, comma 3 del D.P.R. n. 62/2013 ("Codice di comportamento dei di-

pendenti pubblici" e sue modifiche e integrazioni), in ragione del quale andranno evitati situazioni o comportamenti che possano nuocere agli interessi e all'immagine dell'ENEA.

B) L'uso di qualsiasi sistema di comunicazione attraverso l'infrastruttura informatica dell'ENEA è da finalizzare esclusivamente allo svolgimento delle proprie attività lavorative, in linea con gli scopi istituzionali e nel rispetto degli aggiornamenti giuridici in materia.

C) Nell'utilizzo dei propri account di social media, il dipendente adopera ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all'ENEA. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'ENEA o della Pubblica Amministrazione in generale.

D) Al fine di garantirne i necessari profili di riservatezza, le comunicazioni, afferenti direttamente o indirettamente il servizio, non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

E) ENEA raccomanda di non utilizzare applicazioni di instant messaging, chat, piattaforme di comunicazione e collaborazione unificata forniti dall'ENEA, per fini personali o con Utenti che non fanno parte del personale dell'ENEA e non hanno rapporti lavorativi o professionali con essa. Si ricorda, altresì, che l'utilizzo di applicazioni e piattaforme di messaggistica non fornite o autorizzate dall'ENEA, espone le comunicazioni dell'utente su canali non protetti dalla riservatezza e non garantito dalle policy di sicurezza garantiti della Divisione TERIN-ICT.

**ART.8.** *Uso della Rete Locale, Internet e risorse condivise*

A) L'architettura, la configurazione e le connessioni alla rete dell'ENEA, nonché la strutturazione delle postazioni è responsabilità della Divisione TERIN-ICT, come riportato nella declaratoria ENEA, pertanto, eventuali esigenze di modifiche vanno preventivamente sottoposte alla Divisione TERIN-ICT anche ove le risorse per tali modifiche siano esterne alla Divisione stessa.

B) Di norma, ogni postazione di lavoro è connessa alla rete locale ENEA. Agli utenti sono fornite le credenziali per l'accesso, secondo i profili di attribuzione assegnati, a tutti i servizi, alla rete intranet, ad internet ed alle risorse di rete condivise, funzionali all'attività lavorativa. Tali accessi devono avvenire per finalità istituzionali, strettamente connesse agli incarichi lavorativi attribuiti dal proprio Responsabile e sempre nel rispetto delle regole elencate in questo documento.

C) Per l'uso dei servizi connessi ad internet, alla rete locale ed alle risorse di rete condivise, valgono le seguenti regole:

1) la navigazione in Internet deve essere finalizzata allo svolgimento della propria attività lavorativa e in linea con gli scopi istituzionali dell'ENEA; non si devono trasferire sulla propria postazione di lavoro, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento della medesima postazione e della rete;
2) non si può scaricare e/o scambiare materiale protetto da diritti di proprietà intellettuale senza averne titolo;
3) è vietata ogni forma di registrazione non autorizzata a nome dell'ENEA nonché fornire i dati relativi ad e-mail istituzionale per la registrazione e/o l'accesso a siti i cui contenuti non siano legati all'attività lavorativa.

D) Ad ogni utente e ad ogni servizio/ufficio che ne faccia richiesta, viene assegnato uno spazio sui servizi Cloud (EneaBox, OneDrive, ecc.). Le cartelle presenti nei predetti server sono aree di salvataggio e/o condivisione di informazioni strettamente professionali, e pertanto non devono essere utilizzate per scopi diversi;

E) Sulle unità di rete condivise fornite dalla Divisione TERIN-ICT vengono svolte regolari attività di amministrazione e backup; in caso di perdita dei dati è possibile aprire un ticket per tentare di recuperare i dati mancanti.

F) ENEA raccomanda fortemente ai propri dipendenti di utilizzare i sistemi cloud messi a disposizione dalla Divisione TERIN-ICT al fine di salvaguardare l'integrità della rete, la tutela dei dati e del know-how dell'ENEA. L'utilizzo di piattaforme cloud non gestite dalla Divisione TERIN-ICT, non espressamente autorizzate, può esporre l'utente a responsabilità dirette su eventuali violazioni e/o compromissioni di rete e/o dati.

**ART.9.** *Profili, Credenziali e Password*

A) I profili di abilitazione all'utilizzo delle risorse di rete sono collegati all'attività lavorativa svolta e vengono assegnate al dipendente, di concerto con la Divisione TERIN-ICT, sulla base della richiesta di abilitazione provenienti dalle strutture di Enea competenti sullo specifico profilo/servizio.

B) Le credenziali (nome utente e password) per l'accesso ai servizi informatici, anche attraverso i sistemi di autenticazione federata (IDEM, EDUROAM), vengono rilasciate dalla Divisione TERIN-ICT. L'utente deve essere consapevole del fatto che cedere le proprie credenziali, ovvero permettere a terzi l'accesso ai servizi ENEA, significa autorizzarli a proprio nome alla gestione degli stessi, con effetti potenzialmente molto critici (ad es. visualizzazione di informazioni riservate, alterazione o distruzione di dati, uso della propria posta elettronica etc.), e che ciò

potrebbe comportare responsabilità disciplinari per il dipendente nonché responsabilità amministrative, contabili e penali a carico di entrambi i soggetti. È, quindi, severamente vietato cedere a terzi le proprie credenziali.

C) Per una corretta gestione delle credenziali è necessario osservare le seguenti regole:
   a) modificare alla prima connessione la password che è stata fornita;
   b) usare nella composizione della password una sequenza di caratteri, numeri e simboli adeguatamente complessa (è altamente consigliato utilizzare 12 caratteri alfanumerici);
   c) modificare la password almeno ogni anno. Per alcune applicazioni particolarmente critiche è opportuno aggiornare la password per periodi più brevi. Nel caso in cui si abbia conoscenza di un accesso abusivo o si ritenga che la propria password sia stata compromessa, modificarla immediatamente e segnalare l'evento al SOC ed al DPO;
   d) comunicare tempestivamente alla Divisione TERIN-ICT trasferimenti di Unità e cessazioni, in modo da consentire la disabilitazione dell'accesso ai servizi non strettamente necessari ovvero l'attribuzione della nuova profilazione.

D) Le password sono personali e riservate; si fa presente che in caso di prolungata assenza o impedimento dell'utente, ove si renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile di Struttura dell'utente può richiedere alla Divisione TERIN-ICT l'accesso alle informazioni protette dandone tempestiva comunicazione all'utente interessato.

## CAPITOLO 3 CESSAZIONE DEL RAPPORTO DI LAVORO

**ART.10.** *Cessazione del Rapporto*

Al momento della cessazione del rapporto di lavoro, ovvero di qualunque evento che comporti la modifica delle funzioni precedentemente espletate, l'utente deve mettere a disposizione dell'ENEA tutte le risorse assegnate, sia in termini di attrezzature informatiche che di informazioni di interesse per ENEA.

**ART.11.** *Fase di Cessazione*

La fase di Cessazione prevede le seguenti modalità operative:

A) Le credenziali fornite all'utente verranno disabilitate: è cura della Direzione PER comunicare le cessazioni degli utenti alla Divisione TERIN-ICT.
B) La casella di posta elettronica individuale verrà parzialmente disattivata (potrà solo ricevere e inviare una mail automatica di risposta indicante un eventuale nuovo indirizzo personale a cui scrivere) e decorsi dodici mesi sarà cancellata; le attività necessarie per il passaggio delle consegne e le copie del materiale di eventuale interesse del Servizio/Ufficio dovranno essere effettuate prima della disattivazione a cura del Responsabile dell'Unità interessata.
C) Le eventuali registrazioni su siti e sistemi esterni, effettuate per motivi di servizio e legate alla casella di posta elettronica del dipendente, dovranno essere portate a conoscenza del Responsabile diretto in tempo utile per consentire una loro migrazione verso altri utenti, ovvero la loro disabilitazione. A tal proposito si invita ad eseguire tali registrazioni usando indirizzi di posta specifici (di servizio e non personali).
D) Le informazioni e i documenti prodotti o entrati nella disponibilità dell'utente nell'esercizio dell'attività lavorativa a favore dell'ENEA restano nella piena ed esclusiva disponibilità dell'ENEA. L'utente non può ottenere copia e/o cancellare documenti ed informazioni di interesse dell'ENEA presenti sulle Postazioni di Lavoro o sulle risorse di rete, né farne alcun uso dopo la cessazione del rapporto di lavoro, a meno di formale autorizzazione da parte del Responsabile di Unità.
E) Le informazioni eventualmente registrate sulle Postazioni di Lavoro o sulle risorse di rete che non siano di interesse per l'ENEA verranno cancellate al termine del rapporto di lavoro senza alcuna responsabilità per ENEA.

## CAPITOLO 4 INTERVENTI DI ASSISTENZA E MANUTENZIONE

**ART.12.** *Assistenza e manutenzione*

A) Il personale della Divisione TERIN-ICT ha tra i suoi compiti quello di garantire il buon funzionamento generale dell'infrastruttura informatica, assunto il rispetto del presente *Disciplinare ICT* da parte dei singoli utenti e dai Responsabili degli stessi. A tal fine, dedica le proprie risorse in via prioritaria allo svolgimento di tali attività.

B) Gli interventi di supporto su dispositivi informatici non ENEA non possono essere effettuati.

C) Il supporto tecnico è garantito per le configurazioni autorizzate e per i software ufficialmente distribuiti.

## CAPITOLO 5 VERIFICHE, RESPONSABILITA' E SANZIONI

**ART.13.** *Verifiche*

Fermo restando quanto già riportato nei paragrafi precedenti in materia di comportamento in servizio, si fa presente quanto segue:

A) ENEA, utilizzando sistemi informativi centralizzati può avvalersi, nel rispetto dell'art. 4, comma 2 dello Statuto dei Lavoratori, di applicazioni o soluzioni informatiche che permettano un'attività di analisi indiretta a distanza (controllo preterintenzionale affidato al SOC) e determina un trattamento di dati riferiti o riferibili ai lavoratori, nel rispetto delle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la protezione dei Dati Personali in data 1° marzo 2007.

B) ENEA non effettua, in alcun caso, trattamenti di Dati Personali mediante sistemi informatici che mirino al controllo a distanza dei lavoratori, tramite i quali sia possibile ricostruire la loro attività, per esempio mediante l'esecuzione di controlli prolungati, costanti o indiscriminati attraverso l'uso di strumenti elettronici.

C) Il controllo anonimo di cui al precedente comma A) può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti dell'ENEA e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

D) Tutti i log, i dati di traffico sulla rete, i dati relativi al traffico del servizio di Posta Elettronica vengono utilizzati, verificati e conservati dal SOC per un tempo non superiore a 7 giorni al solo

scopo di intervenire prontamente in caso di evidenze di attacchi informatici o usi impropri della rete e/o dei servizi.

**ART.14.** *Responsabilità e sanzioni*

L'inosservanza delle norme descritte nel presente *Disciplinare ICT*, costituisce violazione degli articoli 3, comma 3 del citato D.P.R. 62/2013, del Codice di comportamento dell'ENEA e art. 23, comma 3, lettera a), Titolo V del CCNL Istruzione e Ricerca 2019-2021, ed è fonte di responsabilità disciplinare accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni e può comportare l'applicazione delle sanzioni disciplinari previste dal D.Lgs. n. 165/2001 s.m.i., dal CCNL Istruzione e Ricerca 2019-2021 e dal singolo contratto di lavoro. Resta ferma la responsabilità civile, amministrativa, penale e contabile per fatti illeciti e/o danni derivanti da usi non consentiti della Rete o degli strumenti informatici messi a disposizione dall' ENEA, anche alla luce delle prescrizioni contenute nel presente disciplinare.

## CAPITOLO 6 NORME FINALI

**ART.15.** *Norme finali*

Il *Disciplinare ICT* diventa il riferimento per la revisione di tutte le circolari applicative attualmente in essere e potrà essere aggiornato periodicamente in relazione all'evoluzione tecnologica, organizzativa e della normativa di settore.

# ALLEGATO 1 - NORMATIVA DI RIFERIMENTO NAZIONALE E INTERNA

## *NORMATIVA NAZIONALE*

a. Costituzione della Repubblica Italiana, artt. 15[1], 28[2] (dispone che:);

b. La Legge 20.5.1970, n. 300, recante "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"* (nel proseguo per brevità: "*Statuto dei lavoratori"*);

c. Il Regio Decreto 16 marzo 1942, n. 262 ("*Codice civile*"), in particolare il Libro V, gli *artt.2104[3] e 2105[4];*

d. Codice penale, artt. 616[5], 617-quater[6], 617-quinquies[7], 617-sixier[8]*;*

e. La normativa in materia di *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio* introdotta con la Legge 22 aprile 1941 n. 633, come modificata dal D. Lgs. 29 dicembre 1992, n. 518. Normativa in *attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore*. Tale provvedimento normativo ha aggiunto alla Legge n. 633/1941, tra l'altro, l'art. 171-bis, avente ad oggetto la tutela di programmi per elaboratori. L'art. 171- bis, nel testo vigente di cui alla Legge 18 agosto 2000, n. 248 "*Nuove norme di tutela del diritto d'autore*", prevede sanzioni penali a

[1] *Costituzione art. 15: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge"*

[2] *I funzionari e i dipendenti dello Stato e degli enti pubblici sono direttamente responsabili, secondo le leggi penali, civili e amministrative, degli atti compiuti in violazione di diritti. In tali casi la responsabilità civile si estende allo Stato e agli enti pubblici*

[3] *Art. 2104 c.civ. Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.*

[4] *Art. 2105 c.civ. Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.*

[5] Cod.pen.616: "*Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da trenta euro a cinquecento sedici euro. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza"*

[6] Cod.pen.617-quater: *"Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.*
*Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.*

[7] Cod.pen.617-quinquies: *"Chiunque, fuori dei casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater."*

[8] Cod.pen.617-sixier *Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.*

carico di coloro che duplicano, detengono, distribuiscono o vendono programmi per elaboratore oggetto di diritto d'autore; la norma dispone, quindi, il divieto assoluto di fare copie illegali di materiale protetto da leggi a tutela del diritto d'autore e di rendere tale materiale disponibile a terzi per effettuarne delle copie;

f. Il Regolamento (UE) 2016/679 del 27 aprile 2016: "*General Data Protection Regulation*" (nel proseguo per brevità: "*GDPR*"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;

g. La Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei Dati Personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche);

h. Il D. Lgs. 196/2003 (nel proseguo per brevità: "*Codice della Privacy*") così come modificato dal D. Lgs. 101/2018 e s.m.i.; e segnatamente il Titolo X "*servizi di comunicazione elettronica*" (artt. 121 e ss.); art. 167 (*Trattamento illecito di dati*); 167 bis (*Comunicazione e diffusione illecita di Dati Personali oggetto di trattamento su larga scala*); art. 167- ter (*Acquisizione fraudolenta di Dati Personali oggetto di trattamento su larga scala*); art. 168 (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*);

i. Le "*Linee guida del Garante Privacy* (oggi Garante per la Protezione dei Dati Personali, nel proseguo per brevità: "*Garante*") *per posta elettronica e internet*" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

j. Il 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 AdS",* pubblicato in G.U. n. 300 del 24-12-2008, così come integrato e modificato dalle: *"Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di AdS e proroga dei termini per il loro adempimento - 25 giugno 2009"* pubblicato in G.U. n. 149 del 30 giugno 2009;D. Lgs. 30 marzo 2001, n. 165 e, in particolare, il suo Titolo IV;

k. D. lgs. 82/2005 (Codice dell'amministrazione digitale);

l. Circolare Agenzia per l'Italia Digitale 18 aprile 2017, n. 2/2017 "*Misure minime di sicurezza ICT per le pubbliche amministrazioni* (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)";

m. Legge 20 novembre 2017, n. 167, art. 24, richiamato dall'art. 132 comma 5 bis del Codice Privacy;

n. Legge 3 agosto 2007, n. 124, Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto;

o. DPCM 6 novembre 2015, n. 5, Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva;

p. DPCM 12 giugno 2009, n. 7, Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica;

q. Decreto del Presidente del Consiglio dei ministri 15 giugno 2021: "Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";

r. Agenzia per la Cybersicurezza Nazionale - Circolare 21 aprile 2022, n. 4336. Attuazione dell'articolo 29, comma 3, del decreto-legge 21 marzo 2022, n. 21. Diversificazione di prodotti e servizi tecnologici di sicurezza informatica;

s. Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022; relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abrogala Direttiva (UE) 2016/1148 (direttiva NIS 2). (*cfr. considerato 36 – attività di ricerca*);

t. DPR 16 aprile 2013, n. 62 "Codice di comportamento dei dipendenti pubblici a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165", come modificato dal DPR 13 giugno 2023, n. 81;

u. CCNL Istruzione e Ricerca 2019-2021, Titolo V "Responsabilità disciplinare".

***NORMATIVA INTERNA ENEA***

A. CCNL Istruzione e Ricerca 2019-2021;

B. (AUP) Acceptable Use Policy del Consortium GARR (link: https://www.garr.it/it/regole-di-utilizzo-della-rete-aup);

C. Codice di comportamento dei dipendenti dell'ENEA;

D. Regolamento per l'applicazione del telelavoro e del lavoro agile in ENEA.