REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI DI LAVORO E DEI SISTEMI IT DEL CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI (CNIT)

PRESCRIZIONI PER LA SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI

Versione: ottobre 2026

Sommario

1. Destinatari del documento....4
2. Scopo del documento....4
3. Definizioni....4
4. Indicazioni generali per i dipendenti e per i collaboratori di CNIT....5
   4.1 Conoscenza delle disposizioni in materia di trattamento di dati personali....6
   4.2 Sicurezza di informazioni, dati personali e trattamenti....6
   4.3 Furto/smarrimento di Risorse Informatiche a uso individuale contenenti informazioni di CNIT....6
   4.4 Utilizzo di strumenti gratuiti di I.A. generativa....7
5. Sistema Informativo di CNIT....7
6. Accesso ai Servizi IT di CNIT....8
   6.1 Credenziali utente....8
   6.2 Userid per l'accesso ad ambienti applicativi, alla rete e alla posta elettronica....8
   6.3 Uso delle credenziali utente....8
      6.3.1 Custodia delle credenziali....9
   6.4 Userid tecniche e di amministrazione dei sistemi....9
   6.5 Privilegi di accesso....9
   6.6 Creazione, gestione e dismissione di userid nominative....9
      6.6.1 Creazione e gestione delle credenziali utente di tipo nominativo....9
      6.6.2 Modifica dei privilegi d'accesso....10
      6.6.3 Disattivazione delle Userid nominative....10
      6.6.4 Sospensione/disattivazione temporanea delle Userid nominative....10
      6.6.5 Cessazione del rapporto tra l'assegnatario e CNIT o cambio di mansioni....10
   6.7 Creazione e gestione degli identificativi utente impersonali....10
      6.7.1 Assegnazione delle utenze impersonali....10
      6.7.2 Assenze pianificate o impreviste dell'assegnatario....11
      6.7.3 Assegnazione temporanea delle utenze impersonali....11
      6.7.4 Termine dell'assegnazione temporanea e riassegnazione dell'utenza all'assegnatario....11
      6.7.5 Cessazione del rapporto tra l'assegnatario e CNIT o cambio di mansioni....11
7. Caratteristiche delle password e loro gestione da parte dell'Utente....11
8. Utilizzo delle Risorse informatiche di CNIT....12
   8.1 Cartelle di rete condivise e spazio disco del dispositivo....12
   8.2 Back-up di cartelle e archivi....13
   8.3 Supporti di memorizzazione....13
   8.4 Assegnazione di personal computer / laptop per uso individuale....13

8.5 Dismissione di personal computer 13
8.6 Utilizzo di Personal Computer e laptop (complessivamente PC) 13
8.7 Utilizzo di smartphone e tablet acquistati da CNIT 14
8.8 Cautele nell'utilizzo di dispositivi mobili aziendali (laptop, tablet e smartphone) 14
8.9 Utilizzo e conservazione dei supporti rimovibili 15
9. Documenti cartacei e trattamenti manuali 15
9.1 Gestione e conservazione di documenti cartacei 15
9.2 Trasmissione e riproduzione di documenti cartacei 15
9.3 Smaltimento di documenti cartacei 16
10. Posta elettronica 16
10.1 Periodi di assenza e inoltro automatico 17
10.2 Tempi di conservazione dei log MTA e accesso ai log da parte dell'A.d.S. interno 17
11. Utilizzo dell'account Microsoft 365 17
11.1 Uso di Microsoft Exchange 18
11.2 Uso di Microsoft Teams o di altri strumenti di video-conferenza 18
12. Uso dei Social 18
12.1 Canali e profili social di CNIT 18
12.2 Profili social personali dei dipendenti: contenuti riferiti all'ambito lavorativo 18
13. Navigazione in Internet 19
13.1 Regole generali 19
13.2 Regole esterne alla rete 19
14. Protezione antivirus 20
15. Sistemi di controllo e modalità operative 20
16. Sanzioni 20
17. Storia del documento e revisioni 20

1. Destinatari del documento

Il presente documento è diffuso ai dipendenti e ai collaboratori del Consorzio Nazionale Interuniversitario per le Telecomunicazioni (in breve "CNIT").

2. Scopo del documento

L'utilizzo dei sistemi informativi e della rete aziendale e il libero accesso a Internet dai dispositivi aziendali per lo svolgimento delle attività lavorative può esporre CNIT e i suoi dipendenti e collaboratori a rischi di natura patrimoniale e a responsabilità penali conseguenti alla violazione di specifiche norme di legge (tra le altre legge sul diritto di autore e normativa sulla protezione dei dati personali); può inoltre creare problemi di sicurezza e avere ripercussioni sull'immagine del Consorzio.

Premesso quindi che l'utilizzo delle risorse informatiche, telematiche e telefoniche nell'ambito lavorativo deve sempre ispirarsi al principio della diligenza e correttezza, CNIT ha adottato il presente Regolamento per diffondere la cultura della sicurezza, sottolineare la necessità di tutelare il patrimonio aziendale ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati personali e/o alle informazioni di proprietà di CNIT.

Il presente Regolamento risponde dunque all'esigenza di regolamentare l'utilizzo degli strumenti informatici aziendali e di indicare a dipendenti e collaboratori i comportamenti da adottare, anche attraverso appositi momenti dedicati alla formazione/informazione, al fine di contribuire a garantire la sicurezza informatica del Consorzio, integrando gli obblighi generali di diligenza, correttezza e lealtà previsti dal Codice Etico adottato da CNIT.

Il presente Regolamento non ha limiti temporali di validità, ma potrà essere aggiornato, qualora se ne individuasse la necessità, a seguito di modifiche organizzative di CNIT o di nuove normative generali.

Le principali prescrizioni operative che gli utenti dei sistemi IT dl CNIT sono tenuti a osservare nell'utilizzo delle Risorse Informatiche e dei Servizi IT di CNIT sono riepilogate nell'Allegato 1 – "Prescrizioni per gli Utenti dei sistemi IT del CNIT", che costituisce parte integrante del presente Regolamento.

Eventuali dubbi o richieste di chiarimenti possono essere presentati alla Direzione.

3. Definizioni

Nelle tabelle che seguono sono riportate le definizioni dei principali termini utilizzati nel documento

Protezione dei dati personali	
Termine	**Significato**
Normativa Privacy	Insieme della legislazione sulla protezione dati personali che è composta, a titolo non esaustivo, da: Regolamento Generale sulla Protezione Dati Personali (EU) 2016/679 (GDPR), Dlgs 196/2003 (Codice Privacy), Provvedimenti dell'Autorità Garante per la Protezione Dati Personali, dispositivi di attuazione delle direttive e linee guida europee, Linee guida europee EDPB, Linee guida ENISA sulla protezione delle informazioni, Regolamento e-privacy.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
Responsabile del trattamento	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

Protezione dei dati personali	
Termine	**Significato**
Interessato	Vedere successiva definizione Dati personali
DPO	Responsabile della Protezione dei dati personali designato da CNIT
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Persone autorizzata al trattamento	Personale interno, collaboratori o consulenti autorizzati ad effettuare trattamenti di dati personali sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento in virtù di un contratto/rapporto di lavoro esistente. Nello svolgimento delle attività di trattamento si attengono alle istruzioni ricevute.

Termini descrittivi delle componenti informatiche	
Termine	**Significato**
Utente	La persona fisica (dipendente, dipendente dei partner e Soci, collaboratore o consulente di CNIT) autorizzata all'accesso al Sistema Informativo e agli archivi o a parti degli stessi
Servizi IT	L'insieme delle funzionalità del Sistema Informativo utilizzate da CNIT per lo svolgimento dei propri compiti istituzionali.
Funzione IT interna	Il personale incaricato della gestione del Sistema Informativo e degli archivi di CNIT.
Risorse informatiche di CNIT	L'insieme degli apparati HW (es. server, workstation, laptop, smartphone, stampanti, dispositivi di rete), dei programmi SW (es. applicazioni, librerie di supporto, prodotti o archivi, posta elettronica), delle banche dati e dei servizi internet che permettono di utilizzare correttamente i Servizi IT
Risorsa informatica ad uso individuale	Qualunque risorsa informatica di CNIT assegnata a un singolo utente su richiesta della Direzione, tipicamente un laptop/desktop, una stampante o un archivio personale creato negli spazi di memorizzazione condivisi.
Assegnatario di una risorsa informatica	La persona fisica (dipendente, collaboratore o consulente di CNIT) alla quale sia stata assegnata in dotazione individuale una risorsa informatica per svolgere le mansioni lavorative.
Spazio Disco Utente	Lo spazio di memorizzazione a disposizione dell'Utente per l'archiviazione di materiale in formato elettronico (file)
Amministratore di Sistema	Personale specializzato a cui è conferito l'incarico di provvedere al regolare funzionamento delle Risorse informatiche e del Sistema Informativo CNIT. Lo svolgimento di questo compito può essere affidato a una risorsa interna alla struttura organizzativa di CNIT ("**A.d.S. interno**") o anche, ove applicabile, a un fornitore che dovesse gestire un determinato ambiente di elaborazione per conto di CNIT ("**A.d.S. esterno**").

4. Indicazioni generali per i dipendenti e per i collaboratori di CNIT

I dipendenti devono mantenere la riservatezza sulle informazioni, sui processi interni e sui rapporti con i partner.

La diffusione non autorizzata di informazioni aziendali riservate e di dati personali degli interessati è perseguibile ai sensi del codice civile.

4.1 Conoscenza delle disposizioni in materia di trattamento di dati personali

Qualunque persona autorizzata a svolgere trattamenti di dati personali per conto di CNIT, tenendo conto delle mansioni svolte e del livello di responsabilità assegnato, deve conoscere gli aspetti più rilevanti relativi alla disciplina sulla protezione dei dati personali, i rischi che incombono sui dati e sui trattamenti, le eventuali misure disponibili per prevenire eventi dannosi e i comportamenti da adottare sia nelle operazioni quotidiane sia nelle situazioni di emergenza.

Eventuali situazioni di emergenza non previste dalle procedure dovranno essere inizialmente affrontate con l'obiettivo di ricondurre l'anomalia all'interno di una delle situazioni di emergenza previste.

CNIT mette a disposizione dei dipendenti materiale informativo e percorsi formativi mirati.

I dipendenti ricevono, anche attraverso il presente Regolamento, formazione sull'utilizzo dei dati personali all'interno di CNIT.

Il DPO è disponibile per fornire supporto e chiarimenti.

4.2 Sicurezza di informazioni, dati personali e trattamenti

È obbligatorio rispettare le misure di sicurezza tecniche e organizzative adottate da CNIT, progettate e messe in opera per garantire la riservatezza dei sistemi, delle comunicazioni elettroniche, dei dati personali e delle informazioni aziendali; gli utenti devono altresì essere consapevoli che il tentativo di superare o forzare le misure di sicurezza potrebbe essere interpretato come reato ai sensi del codice penale.

Le operazioni di trattamento di dati personali devono conformarsi alle istruzioni contenute nel presente Regolamento.

Tutti i dati personali trattati da CNIT sono tutelati e protetti e la loro riservatezza è garantita anche attraverso l'adozione e il rispetto dei comportamenti qui richiamati.

Nessuna informazione relativa alle misure di sicurezza applicate – incluse password, credenziali e altri codici di accesso – alle procedure, agli strumenti e ai sistemi utilizzati per effettuare i trattamenti di dati può essere divulgata a terzi.

I dipendenti sono tenuti al rispetto della normativa vigente in materia di fedeltà al datore di lavoro, riservatezza e tutela dei segreti. Detti obblighi rimangono in essere anche dopo la cessazione, per qualsiasi causa e motivo, del rapporto con CNIT.

L'inosservanza delle norme in materia di tutela dei dati personali, nonché delle presenti istruzioni, potrebbe comportare sanzioni e provvedimenti disciplinari, fatta salva ogni altra sanzione di legge (penale, amministrativa, civile) che risultasse applicabile nel caso concreto.

4.3 Furto/smarrimento di Risorse Informatiche a uso individuale contenenti informazioni di CNIT

In caso di furto/smarrimento di risorse informatiche aziendali loro assegnate e di dispositivi contenenti informazioni di CNIT o dati personali dei suoi interessati, l'Utente dovrà:

- avvertire tempestivamente la Direzione, allo scopo di prevenire possibili intrusioni nei Servizi IT eseguite sfruttando le informazioni eventualmente memorizzate sui dispositivi portatili (informazioni relative, ad esempio, alla configurazione del sistema e alle credenziali di accesso dell'assegnatario);
- inviare una e-mail con una breve descrizione dell'accaduto all'indirizzo direzione@cnit.it;
- effettuare la denuncia presso le autorità competenti e inviarne copia alla Direzione per archiviazione.

In caso di furto di supporti informatici contenenti informazioni proprietarie (chiavette USB, dischi esterni) l'Utente dovrà effettuare la denuncia presso le autorità competenti e inviarne copia alla Direzione per archiviazione.

In entrambi i casi, CNIT procederà se possibile alla verifica della tipologia dei dati persi, secondo quanto previsto dalla procedura per la gestione delle violazioni di dati personali.

L'utilizzo dei Servizi IT non conforme a quanto previsto dal presente Regolamento può comportare la sospensione delle credenziali utente e, laddove ne ricorressero gli estremi, a un'eventuale azione legale al fine di tutelare gli interessi di CNIT.

Le risorse informatiche assegnate all'Utente, in forma esclusiva o in condivisione, devono essere utilizzate esclusivamente per scopi leciti connessi con l'attività lavorativa.

4.4 Utilizzo di strumenti gratuiti di I.A. generativa

E' consentito all'Utente l'utilizzo consapevole e corretto di strumenti di I.A. generativa gratuita per scrivere relazioni, documenti, preparare presentazioni, supportare lo sviluppo software mediante la generazione o revisione di codice o analizzare informazioni di CNIT.

L'utilizzo di questi strumenti in ambito lavorativo può presentare i seguenti rischi per CNIT:

- **diffusione di informazioni interne a persone non autorizzate a conoscerle,** in quanto questi strumenti possono utilizzare le informazioni fornite per finalità di training del modello e possono successivamente inserirle, in tutto o in parte, in contenuti forniti ad altri utilizzatori;
- **perdita di riservatezza di dati riferiti a persone fisiche** qualora il prompt contenga anche informazioni personali necessarie alla generazione di determinati contenuti, come potrebbe accadere nel caso di presentazioni interne, relazioni sulle attività o verbali di riunioni;
- **diffusione di codice sorgente, configurazioni, credenziali, chiavi crittografiche, token di autenticazione, documentazione tecnica o altre informazioni relative ai sistemi informativi del CNIT**, con conseguente compromissione della sicurezza, della riservatezza o della proprietà intellettuale;
- **introduzione di codice non sicuro, errato o soggetto a vincoli di licenza incompatibili con le politiche del CNIT**, qualora il codice generato dall'I.A. venga utilizzato senza un'adeguata verifica tecnica.

L'Utente è pertanto tenuto a rispettare alcuni principi fondamentali, previsti dall'Artificial Intelligence Act e dal General Data Protection Regulation (GDPR), tra cui:

- Trasparenza: qualora i contenuti generati mediante sistemi di intelligenza artificiale siano destinati alla diffusione o alla condivisione con terzi (quali, a titolo esemplificativo, relazioni, report, presentazioni, materiale informativo o documentazione tecnica), l'Utente deve indicare, ove appropriato, che tali contenuti sono stati elaborati con il supporto di strumenti di intelligenza artificiale;
- Supervisione Umana: l'Utente è responsabile della verifica, del controllo e della validazione dei contenuti, delle informazioni e del codice generati mediante sistemi di intelligenza artificiale prima del loro utilizzo in documenti ufficiali, comunicazioni, processi decisionali o applicazioni software;
- Protezione dei dati e riservatezza delle informazioni: è fatto divieto di inserire nei sistemi di intelligenza artificiale pubblici o gratuiti dati personali, in particolare se appartenenti a categorie particolari, nonché informazioni riservate, confidenziali o comunque riconducibili all'organizzazione, ivi compresi codice sorgente, configurazioni di sistema, credenziali, chiavi crittografiche, token di autenticazione e documentazione tecnica, salvo nei casi espressamente autorizzati e nel rispetto della normativa vigente.

5. Sistema Informativo di CNIT

Il Sistema Informativo del Consorzio si compone principalmente di:

- **Sistema di posta elettronica,** con credenziali nominative assegnate a dipendenti e collaboratori per la ricezione e l'invio di messaggi da/verso l'interno e da/verso l'esterno (partner, consulenti, ricercatori).
- **Prodotti/piattaforme di informatica individuale**, cioè prodotti di supporto allo svolgimento delle attività assegnate. Si tratta di prodotti standardizzati e spesso preinstallati sul PC aziendale. Oltre alla Suite Microsoft 365, fanno parte di questa classificazione gli strumenti di video-conferenza in uso.
- **Sistemi gestionali e amministrativi**, cioè applicazioni utilizzate per la gestione dei processi amministrativi, contabili, del personale, della rendicontazione dei progetti, degli acquisti, delle missioni, della gestione documentale, del protocollo informatico, della conservazione digitale, della gestione delle identità digitali e degli altri processi istituzionali del Consorzio, solitamente gestiti da fornitori esterni.
- **Applicazioni tecnico-scientifiche e di ricerca,** cioè software e piattaforme utilizzati per le attività di ricerca, sviluppo e innovazione, quali ambienti di sviluppo software, sistemi di controllo versione del codice sorgente, strumenti di gestione dei progetti di ricerca, ambienti di simulazione e calcolo scientifico, piattaforme di High Performance Computing (HPC), sistemi per l'analisi dei dati, strumenti di virtualizzazione e containerizzazione, repository di dati e software, nonché applicazioni specialistiche utilizzate nell'ambito dei progetti di ricerca e delle infrastrutture gestite dal CNIT generalmente gestiti a livello locale dalle Unità di Ricerca che le utilizzano.
- **Archivi utente Condivisi,** cioè archivi contenenti dati trattati da CNIT e gestiti dalla Funzione IT. I dati si trovano su supporti del tipo cartella/Cloud e possono essere consultati e/o aggiornati da più persone, che vi accedono per motivi di lavoro e in base a profili utente stabiliti dalla Direzione congiuntamente con IT.

- **Sito web istituzionale**, cioè l'insieme delle risorse HW e SW che permettono al CNIT di essere raggiungibile sul web.
- **Canali social**, cioè i profili pubblici del CNIT sulle comuni piattaforme di Social Media (YouTube, Linkedin, X, Facebook, Instagram).

Per il ruolo svolto da CNIT, è previsto che alcuni utenti dei servizi possano accedere ad **applicazioni centralizzate di Enti terzi** (es. Ministeri o Commissione Europea) e svolgere operazioni di trattamento per l'esecuzione dei compiti loro assegnate. Queste applicazioni e le relative Banche Dati sono gestite direttamente dall'Ente di riferimento, responsabile delle misure di sicurezza tecniche e organizzative applicabili all'ambiente applicativo di trattamento.

6. Accesso ai Servizi IT di CNIT

L'accesso ai Sistemi IT di CNIT avviene mediante l'utilizzo di credenziali di autenticazione rilasciate al personale e ai collaboratori; l'accesso alle risorse di elaborazione avviene mediante un processo di autenticazione delle **credenziali utente** (codice utente + password) per permettere la verifica dell'identità di chi sta chiedendo l'accesso.

6.1 Credenziali utente

Il codice identificativo assegnato a dipendenti e collaboratori è configurato con un livello di permessi minimo (necessario e sufficiente) allo svolgimento delle mansioni affidate (Principio del "*Need-to-Known*").

Dunque, il processo di autenticazione degli utenti di una specifica componente dei Servizi IT di CNIT si basa in generale su:

- l'attribuzione di un **identificativo utente** (***userid***) alla persona che deve accedere a una determinata componente del Sistema Informatico (**utente**);
- il possesso di una **parola chiave** (***password)*** associata all'identificativo utente, *che* l'assegnatario cambia al primo accesso e custodisce sotto la propria responsabilità;
- un gruppo **di permessi** (***abilitazioni o privilegi di accesso***) attribuiti allo specifico identificativo utente per consentire all'assegnatario di svolgere i compiti di lavoro.

Per gli accessi più critici (Pannello di amministrazione piattaforma cloud Microsoft 365, Pannello di amministrazione sito web istituzionale, ..), CNIT fa uso di strumenti di autenticazione a due fattori, mediante APP di autenticazione sul telefono della risorsa autorizzata, che fanno uso sia di notifiche PUSH che di codici generati ad intervalli regolari per la verifica dell'identità); sono anche previsti appositi codici di recupero, utilizzabili una sola volta, da utilizzare nel caso di smarrimento o malfunzionamento del telefono.

6.2 Userid per l'accesso ad ambienti applicativi, alla rete e alla posta elettronica

L'userid assegnato a dipendenti e collaboratori può essere di **tipo nominativo**, come generalmente avviene per l'accesso alla rete e agli archivi (es. nome.cognome@cnit.it) o di **tipo non nominativo** (es. processo@cnit.it, progetto@cnit.it, o evento@cnit.it) nel caso in cui l'identificativo coincida con un ruolo organizzativo o funzionale (come la gestione di un processo amministrativo, di un progetto di ricerca o un evento) svolto dall'assegnatario all'interno di CNIT.

La **Funzione IT** mantiene un repository storico, ***il Registro delle utenze***, per tracciare la correlazione fra userid e dati anagrafici dell'assegnatario.

6.3 Uso delle credenziali utente

Le credenziali utente (la combinazione di userid e password) sono ad uso strettamente personale e possono essere utilizzate esclusivamente per ragioni di lavoro. L'assegnatario è l'unico responsabile di ogni attività riconducibile all'uso delle credenziali che gli sono state assegnate e deve custodirle adeguatamente per evitare usi non autorizzati dei Servizi IT da parte di terzi.

L'Amministratore di Sistema o un qualunque fornitore che dovesse gestire un determinato ambiente di elaborazione per conto di CNIT non è in alcun modo autorizzato a conoscere/richiedere la password associata all'identificativo utente, se non in caso di necessità particolari, come ad esempio la migrazione dei servizi IT da un

provider all'altro e di esplicite richieste di supporto operativo da parte dell'utente. Esclusivamente in tali evenienze, l'utente è autorizzato a comunicare la propria password all'Amministratore di sistema per l'effettuazione dell'intervento, al termine del quale l'utente è tenuto ad effettuare immediatamente il reset della password.

Gli accessi alle risorse informatiche effettuate dai singoli userid sono tracciati secondo quanto previsto dalla gestione dei **log** (registrazione cronologica e sequenziale delle attività e degli eventi che si verificano in un sistema informatico) prevista per i singoli ambienti applicativi. L'accesso ai log applicativi è effettuato per mezzo degli Amministratori di Sistema e, ove applicabile, avviene nei termini e nei limiti stabiliti nei Data Processing Agreement stipulati con i fornitori.

6.3.1 Custodia delle credenziali

È fatto divieto di memorizzare le credenziali di accesso assegnate sul dispositivo (es. all'interno di file WORD o EXCEL o nella cache del browser utilizzato) o su supporti cartacei, di comunicare ad altre persone le proprie credenziali e di utilizzare le credenziali assegnate ad altri utenti per l'accesso a rete, sistemi e applicazioni.

6.4 Userid tecniche e di amministrazione dei sistemi

Le utenze di amministrazione dei sistemi e le utenze tecniche – rispettivamente quelle necessarie alla gestione dei sistemi e/o delle applicazioni e quelle utilizzate per ragioni di supporto agli utenti, anche da remoto, e per l'acquisizione di permessi necessari alle elaborazioni - sono assegnate in uso all'Amministratore di Sistema e, ove applicabile, ai fornitori che svolgono servizi di gestione e amministrazione di un ambiente applicativo di CNIT.

6.5 Privilegi di accesso

I privilegi di accesso sono associati agli identificativi utente sulla base delle mansioni assegnate e delle attività operative svolte.

Nell'assegnazione dei permessi sono tenuti presenti i seguenti principi:

- il principio della separazione dei compiti;
- il principio del minimo privilegio;
- la necessità di rispettare i vincoli di sicurezza e degli eventuali obblighi di origine legislativa o contrattuale.

I privilegi associati alla userid sono oggetto di verifica periodica della Direzione relativamente alla coerenza con la mansione e le attività dell'assegnatario; per quanto possibile, le abilitazioni devono essere concesse utilizzando ruoli e gruppi di sicurezza.

6.6 Creazione, gestione e dismissione di userid nominative

L'identificativo utente, una volta attribuito, **non potrà essere riassegnato** successivamente ad altri utilizzatori, in quanto legato in modo indissolubile alla persona a cui è stato assegnato e che lo ha utilizzato; una volta creato, non può essere cancellato, con esclusione di *userid* creato in modo erroneo e non ancora nella disponibilità dell'assegnatario.

La userid deve essere tempestivamente disabilitata al venir meno della necessità per cui è stata creata e la necessità di tenerla attiva deve essere oggetto di verifica periodica.

6.6.1 Creazione e gestione delle credenziali utente di tipo nominativo

La **Direzione**, all'inizio di un nuovo rapporto di lavoro o di un nuovo rapporto di collaborazione, richiede **alla Funzione IT** ovvero, ove applicabile, al fornitore che gestisce una specifica componente o un determinato servizio applicativo, la creazione delle userid che saranno assegnate alla persona in questione, quali ad esempio l'utenza di dominio e le userid per l'accesso all'ambiente applicativo e alla posta elettronica.

La richiesta, inviata via email dalla Funzione IT, specifica gli elementi identificativi dell'assegnatario (nome, cognome, …), le abilitazioni da attribuire alla userid, e, se rilevante, la data in cui termina il rapporto con CNIT, nel caso ad esempio di contratto a tempo determinato o di incarico a termine per un consulente.

La Funzione IT / il Fornitore :

- crea la/e userid richieste e la password per il primo accesso con le abilitazioni richieste;
- risponde alla mail, comunicando le credenziali di accesso create (*userid* e *password iniziale*).

- consegna le credenziali di dominio e quelle applicative all'assegnatario;
- aggiorna il ***Registro delle Utenze***, indicando per ciascun assegnatario le userid attribuite.

6.6.2 Modifica dei privilegi d'accesso

Nel caso in cui le mansioni assegnate all'assegnatario richiedano un adeguamento delle abilitazioni associate alla userid, **la Direzione**, con le stesse modalità illustrate al punto precedente, richiede la variazione fornendo tutte le informazioni necessarie all'esecuzione delle attività, specificando la data entro la quale dovrà avere effetto la modifica.

La Funzione IT / il Fornitore:

- varia le abilitazioni entro la data prevista;
- risponde alla mail, comunicando il completamento dell'attività.

6.6.3 Disattivazione delle Userid nominative

Al termine del rapporto di lavoro o del rapporto contrattuale tra CNIT e l'assegnatario di userid la **Direzione**, con le stesse modalità operative illustrate al precedente punto 6.6.1, chiede la disattivazione delle credenziali di accesso, avendo cura di specificare la data in cui tale disattivazione deve essere effettiva.

La **Funzione IT** / **il Fornitore**, per il proprio ambito di responsabilità, disattiva la userid alla data richieste e comunica via mail alla **Direzione** il completamento dell'attività; aggiorna inoltre il ***Registro delle Utenze***, inserendo la data di cessazione delle userid.

6.6.4 Sospensione/disattivazione temporanea delle Userid nominative

In caso di assenza prolungata dal lavoro dell'assegnatario la **Direzione**, con le stesse modalità operative illustrate al precedente punto 6.6.1, può richiede la disattivazione delle credenziali di accesso, avendo cura di specificare la data in cui tale disattivazione deve essere effettiva.

L'Amministratore di Sistema, per il proprio ambito di responsabilità, disattiva la userid alla data richieste e comunica via mail alla Funzione IT il completamento dell'attività.

La **Funzione IT** aggiorna il ***Registro delle Utenze***, inserendo la data di sospensione delle userid.

Con le stesse modalità operative, al rientro al lavoro dell'assegnatario, la Direzione chiede di riattivare le credenziali sospese e comunica al rientrante la nuova password per il primo accesso.

La **Funzione IT** aggiorna il ***Registro delle Utenze***, inserendo la data di riattivazione delle userid.

6.6.5 Cessazione del rapporto tra l'assegnatario e CNIT o cambio di mansioni

Qualora, per qualunque motivo, il rapporto in essere tra l'assegnatario CNIT si concluda, le suddette utenze personali saranno eliminate entro i 90 giorni successivi e non saranno assegnate ad altro Utente.

6.7 Creazione e gestione degli identificativi utente impersonali

Come specificato al precedente paragrafo 6.2, alcuni identificativi utente assegnati per l'accesso alle caselle di posta elettronica sono di tipo impersonale.

L'utilizzo e la gestione delle userid impersonali è assegnata a dipendenti e collaboratori sulla base del compito svolto all'interno della struttura organizzativa.

Le userid non sono quindi appositamente create ma sono pre-fissate e non sono dismesse quando il dipendente che le ha in assegnazione interrompe, per qualunque motivo, il proprio rapporto con CNIT.

Nei paragrafi che seguono si forniscono informazioni sulla modalità di gestione delle userid impersonali; la gestione del sistema di posta elettronica di CNIT è assegnata alla Funzione IT.

6.7.1 Assegnazione delle utenze impersonali

La Direzione CNIT, all'inizio di un nuovo rapporto di lavoro o di un nuovo rapporto di collaborazione, notifica via email alla Funzione IT il nuovo assegnatario della casella email, specificando gli elementi identificativi dell'assegnatario (nome, cognome) e la data di assegnazione della specifica userid.

La **Funzione IT** consegna le credenziali all'assegnatario e aggiorna il **Registro delle Utenze**.

6.7.2 Assenze pianificate o impreviste dell'assegnatario

In caso di assenza imprevista prolungata o in casi del tutto eccezionali e motivati (es. scadenze impellenti), la Direzione indicherà alla Funzione IT il nominativo della persona temporaneamente delegata all'accesso alla casella email (cfr. successivo paragrafo 6.7.3), specificando il/i relativo/o identificativo/i utente e i dati anagrafici e l'indirizzo email dell'assegnatario pro-tempore.

6.7.3 Assegnazione temporanea delle utenze impersonali

La Direzione concorda con la Funzione IT interno la data e l'ora della riassegnazione; e la Funzione IT dà seguito alla richiesta e comunica all'assegnatario pro-tempore le credenziali di accesso; raccomanda inoltre all'assegnatario pro-tempore il dovere di rispettare la privacy per le informazioni personali di cui eventualmente dovesse venire a conoscenza nell'utilizzo della casella email.

La Funzione IT aggiorna il **Registro delle Assegnazioni Temporanee** specificando la data di assegnazione e il motivo che l'ha resa necessaria; l'assegnazione temporanea si interrompe al cessare dell'esigenza che l'ha determinata.

6.7.4 Termine dell'assegnazione temporanea e riassegnazione dell'utenza all'assegnatario

Al termine della situazione eccezionale o al rientro dell'assegnatario in ufficio, la Direzione richiede un intervento, finalizzato alla riassegnazione della/e utenza/e all'assegnatario; la **Funzione IT** aggiorna di conseguenza il **Registro delle Assegnazioni Temporanee**.

6.7.5 Cessazione del rapporto tra l'assegnatario e CNIT o cambio di mansioni.

Qualora, per qualunque motivo, il rapporto in essere tra l'assegnatario CNIT si concluda, le suddette utenze impersonali saranno assegnate al subentrante nel ruolo o assegnate pro-tempore a un sostituto fino all'individuazione del nuovo assegnatario.

In caso di cessazione del rapporto di lavoro o di cambio di mansione, l'identificativo utente per l'accesso alla casella di posta elettronica e l'intero contenuto della stessa sono trasferiti al subentrante nel ruolo o al facente funzioni pro-tempore.

7. Caratteristiche delle password e loro gestione da parte dell'Utente

La password deve rispettare i requisiti definiti da CNIT per l'accesso alle diverse componenti IT in termini di lunghezza minima, complessità, scadenza e riutilizzabilità.

La password comunicata all'assegnatario per il primo accesso (**password iniziale**) deve essere obbligatoriamente modificata dall'assegnatario al primo utilizzo; in caso di dimenticanza della password, devono essere implementati meccanismi che consentano all'Utente il **reset** della password o devono essere previsti meccanismi alternativi basati sull'identificazione certa dell'Utente.

I meccanismi di gestione della password prevedono:

- la mascheratura dei caratteri della password durante la digitazione;
- la sostituzione autonoma della password da parte dell'Utente;
- la protezione dell'archivio delle password per impedire accessi da parte di persone non autorizzate;
- l'utilizzo di tecniche di cifratura per trasmettere userid e password in rete;
- la sospensione dell'utenza di dominio dopo un numero massimo predefinito di tentativi di accesso falliti.

I meccanismi di autenticazione devono garantire un livello di sicurezza coerente con la criticità delle informazioni di CNIT, utilizzando, ove previsto, criteri di autenticazione a due fattori (Multi Factor Authentication - MFA).

Al primo accesso ai sistemi, l'Utente deve cambiare la password ricevuta; non è consentito utilizzare la stessa password per accedere a più servizi/applicazioni, cioè in associazioni a più userid.

È richiesto che la password impostata dall'Utente abbia le seguenti caratteristiche:

a) è composta utilizzando lettere minuscole e maiuscole, numeri e caratteri speciali;
b) ha una lunghezza minima di 8 caratteri ma è preferibile, se il sistema lo ammette, impostare password di lunghezza pari a 12 caratteri;
c) non deve contenere elementi facilmente riconducibili all'Utente (come, ad esempio, nomi di componenti del nucleo familiare, inclusi animali di famiglia, o date di nascita) e non deve essere uguale alla userid;

d) deve essere diversa dalle 5 cinque precedentemente usate.

La custodia della password è una precisa responsabilità dell'Utente, che deve adoperarsi per mantenerla riservata. Alla custodia della password, che è una componente delle credenziali d'accesso ai Sistemi IT, si applicano le indicazioni fornite al punto 6.3.1.

L'Utente deve immediatamente modificare la password se ha il sospetto che qualcuno possa averla individuata, anche nel caso in cui i termini di validità della stessa non siano scaduti.

8. Utilizzo delle Risorse informatiche di CNIT

Quando utilizza le Risorse Informatiche, l'Utente è tenuto al pieno rispetto della normativa vigente e alle indicazioni fornite da CNIT con questo documento.

8.1 Cartelle di rete condivise e spazio disco del dispositivo

Per l'accesso alle risorse di CNIT l'Utente deve essere in possesso della specifica credenziale di autenticazione.

Le cartelle condivise sono aree di divulgazione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, nessun file che non sia legato all'attività lavorativa può essere dislocato, nemmeno per brevi periodi, in queste unità.

È fortemente consigliato all'Utente di non memorizzare documenti aziendali sul disco fisso della postazione di lavoro in dotazione ma di salvare tutti i documenti prodotti nello svolgimento delle proprie mansioni e rilevanti per l'attività di lavoro nelle cartelle condivise appositamente predisposte.

Poter disporre di un archivio centralizzato ha numerosi vantaggi dal punto di vista della protezione dei dati personali, in quanto permette di avere a disposizione dati esatti e aggiornati e di proteggere meglio la loro integrità e riservatezza; la memorizzazione in archivi locali di eventuali copie, copie parziali o file che sono il risultato di elaborazioni dell'Utente rende difficile tenere traccia della presenza di dati personali in archivi non strutturati e può esporre CNIT al rischio di rispondere in modo inesatto o incompleto a richieste avanzate dagli interessati in merito ai propri dati personali (es. richiesta di accesso ai dati o di cancellazione dei dati).

È necessario che ogni Utente sia consapevole delle possibili conseguente per il CNIT legate al proliferare di archivi non strutturati.

La memorizzazione di dati personali in archivi locali deve quindi essere limitata allo stretto necessario e motivata da ragioni strettamente legate alla mansione svolta.

Pertanto, ogni Utente è responsabile di:

- memorizzare in locale, solo per stringenti e motivate necessità di lavoro, esclusivamente i dati personali necessari all'attività da svolgere, così da ridurre al minimo la conservazione di dati personali nel disco fisso della postazione di lavoro assegnata;
- effettuare revisioni periodiche (almeno ogni tre mesi) degli archivi locali, provvedendo alla loro pulizia, con cancellazione dei file obsoleti o non più utili per lo scopo per il quale sono stati creati;
- non trasmettere ai colleghi file contenenti dati personali di interessati attraverso la posta elettronica; è preferibile inviare ai colleghi che hanno bisogno di accedere ai dati il link alla cartella condivisa, evitando il proliferare di ulteriori copie locali.

Nessun file di carattere personale può essere memorizzato nello Spazio disco della postazione di lavoro assegnata; in ogni caso, non è consentito conservare in locale documenti (indipendentemente dal fatto che in essi siano presenti dati personali) con estensione file non riconosciuta dai sistemi di CNIT.

Per esigenze di servizio legate esclusivamente alla gestione delle Risorse Informatiche, l'A.d.S. interno potrà avere accesso allo Spazio Disco Utente. Nel caso ciò avvenisse, l'A.d.S. interno:

- manterranno riservate le informazioni, relative all'Utente, di cui potrà venire a conoscenza durante l'Accesso, fatta eccezione per quanto previsto e richiesto dalla Legge;
- per gli accessi regolati dal presente Regolamento non si potrà in alcun modo configurare per l'A.d.S. interno una violazione di quanto disposto dalla normativa vigente sulla protezione dei dati personali.

8.2 Back-up di cartelle e archivi

I file memorizzati nell'apposita piattaforma di collaborazione e condivisione non sono oggetto di backup automatico. Eventuali soluzioni di backup potranno essere oggetto di valutazione nel futuro.

La responsabilità del salvataggio e del backup dei dati sia sugli archivi locali che sulle cartelle condivise in rete è pertanto a carico del singolo Utente.

L'A.d.S. interno può procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sul PC assegnato all'Utente sia sulle unità condivise, preallertando la Direzione e l'Utente interessato.

8.3 Supporti di memorizzazione

I supporti informatici (dischi zip, dischi fissi di personal computer, dischi ottici, etc.) contenenti o che hanno contenuto dati personali possono essere riutilizzati (per registrare altri dati, per inviare dati a corrispondenti interni o esterni, per prestare il supporto informatico ad altri, etc.) solo previa cancellazione permanente (es.: riformattazione completa) del supporto stesso.

La riformattazione veloce o la semplice cancellazione dei file non sono sufficienti. I supporti digitali contenenti dati personali non utilizzati od utilizzati che non siano destinati a conservazione devono essere distrutti. Per indicazioni sulla cancellazione permanente si faccia riferimento alla Funzione IT.

8.4 Assegnazione di personal computer / laptop per uso individuale

Non è consentito trasferire un personal computer da un assegnatario ad un altro senza informare la Funzione IT, che in tal caso provvederà a riformattare il disco fisso o a cancellare i dati in esso contenuti in modo da renderli tecnicamente non recuperabili e a cambiare la password del personal computer.

Quando un personal computer individuale (nuovo o proveniente da un precedente assegnatario) è consegnato a un assegnatario, la Funzione IT attiva l'opzione di protezione tramite password di personal computer e comunica tale password all'assegnatario. L'Utente è forzato dal sistema a cambiare la password dopo il primo accesso.

8.5 Dismissione di personal computer

Quando un assegnatario dismette un personal computer a lui assegnato (per dimissioni, pensionamento, cambio di incarico ecc.), la Funzione IT provvede, se necessario, a fare una copia dei file, ad esclusione dei file designati come "personali" dall'assegnatario cessante e non cancellati dallo stesso, presenti nel disco fisso, su CD-ROM o supporto di salvataggio non riscrivibile, conservandolo in luogo sicuro.

L'eventuale accesso ai dati salvati è autorizzato per iscritto dall'assegnatario della risorsa informatica.

8.6 Utilizzo di Personal Computer e laptop (complessivamente PC)

Il PC assegnato all'Utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi e, soprattutto, causare minacce alla sicurezza.

La configurazione HW e SW del PC non può essere modificata dall'Utente senza autorizzazione.

L'Utente deve custodire il PC a lui assegnato con diligenza, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati/autorizzati da CNIT, né è consentito all'Utente di installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza della presente disposizione può esporre CNIT a responsabilità civili o anche penali, in quanto le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, sono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione della Direzione e della Funzione IT, l'Utente non può modificare le caratteristiche impostate sul PC né installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.); deve inoltre prestare la massima attenzione ai supporti di origine esterna (pendrive usb, cavi per la ricarica dei dispositivi, etc.), avvertendo immediatamente la Funzione IT nel caso in cui rilevati virus o ne sospetti l'esistenza.

Il PC deve essere spento in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo.

È previsto l'uso di screensaver a tempo (5 minuti), con l'obbligo di reintrodurre la password per l'accesso una volta che lo screen saver si sia attivato.

Non è consentito all'Utente di modificare le funzioni e gli aggiornamenti di sicurezza gestiti dalla Funzione IT.

Il personale della Funzione IT ha la facoltà di collegarsi e visualizzare in remoto il desktop dei PC al fine di garantire l'assistenza tecnica e la normale attività operativa. L'intervento è effettuato esclusivamente su richiesta dell'Utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nei Sistemi IT di CNIT e nelle connessioni di rete.

8.7 Utilizzo di smartphone e tablet acquistati da CNIT

L'Utente è responsabile dello strumento di lavoro mobile (smartphone e tablet) assegnatogli dalla Società e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Precisando che le operazioni effettuate mediante smartphone e tablet sono di responsabilità dell'Utente a cui sono stati assegnati, il corretto utilizzo di questi strumenti prevede il rispetto delle seguenti regole:

Agli smartphone e tablet si applicano le seguenti regole:

- le applicazioni scaricabili tramite App Store di Apple / Play Store di Google sono da considerarsi sicure nei limiti della ragionevolezza; è pertanto richiesto di scaricare solo APP necessarie allo svolgimento e alla semplificazione dell'attività di lavoro;
- è fatto divieto di modificare i dispositivi mobili tramite manipolazione software e l'installazione di applicazioni non appartenenti ad App store dei produttori;
- i dispositivi mobili devono essere protetti da un codice di quattro cifre (minimo) e da impronta digitale se questa funzionalità è presente;
- l'utilizzo di APP di messagistica è consentito solo per necessità stringenti (richiesta di essere contattati, urgenze); la trasmissione di file o archivi contenenti informazioni o dati personali gestiti da CNIT con questi strumenti non è consentita.

Per quanto concerne il servizio di fonia mobile assegnato all'Utente, lo stesso si impegna a non utilizzare il servizio per:

- trasmettere o diffondere contenuti che siano illeciti, dannosi, minatori, abusivi, molesti, diffamatori e/o calunniosi, volgari, osceni, lesivi della privacy altrui, razzisti, classisti o comunque reprensibili;
- arrecare danno, in qualsivoglia modo, a minori di età;
- falsificare la propria identità presentandosi o in altro modo mentire circa il proprio rapporto con altri soggetti;
- manipolare segni distintivi o indicazioni al fine di contraffare l'origine di un contenuto trasmesso o diffuso tramite il servizio di fonia mobile;
- trasmettere o diffondere un contenuto che non abbia il diritto di trasmettere o diffondere in forza di una previsione di legge, di contratto ovvero a causa di un rapporto fiduciario (per esempio informazioni riservate, informazioni confidenziali apprese in forza di un rapporto di lavoro o protette da un patto di riservatezza);
- trasmettere o diffondere un contenuto che comporti la violazione di brevetti, marchi, segreti, diritti di autore o altri diritti di proprietà industriale e/o intellettuale di CNIT, dei suoi partner o di soggetti terzi;
- trasmettere o diffondere pubblicità, materiale promozionale, catene, piramidi, o qualsiasi altra forma di sollecitazione non autorizzate o non richieste;
- perseguitare o in altro modo molestare soggetti terzi.

8.8 Cautele nell'utilizzo di dispositivi mobili aziendali (laptop, tablet e smartphone)

I dispositivi mobili assegnati all'Utente:

- non devono essere utilizzati in contesti in cui persone non autorizzate possono entrare in contatto con informazioni di CNIT o con i dati personali trattati;

- devono essere utilizzati con estrema attenzione quando altre persone (osservatori) possono entrare in contatto, anche occasionalmente (viaggi in treno, autobus, aereo …), con il contenuto delle pagine, che potrebbero contenere dati personali o informazioni aziendali riservate;
- non devono essere lasciati incustoditi in luoghi pubblici, per nessun motivo;
- il loro utilizzo non deve essere permesso a persone non autorizzate a usare le informazioni aziendali;
- l'accesso al dispositivo deve avvenire a seguito di autenticazione di credenziali, o codici o riconoscimenti biometrici secondo gli standard utilizzati dallo strumento.

8.9 Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali nonché informazioni costituenti know-how di CNIT o dei suoi afferenti, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun Utente dovrà contattare la Funzione IT e seguire le istruzioni da questa impartite.

In ogni caso, i supporti rimovibili contenenti dati personali devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

È vietato l'utilizzo di supporti rimovibili personali non preventivamente autorizzati dalla Direzione.

L'Utente è responsabile della custodia dei supporti e del loro contenuto.

9. Documenti cartacei e trattamenti manuali

I trattamenti di dati personali possono avvenire in modalità manuale.

Sono considerate operazioni di trattamento manuali la raccolta di documenti cartacei, la loro riproduzione fotostatica, la stampa di documenti elettronici e le eventuali ulteriori elaborazioni di tali documenti per costituire un archivio.

9.1 Gestione e conservazione di documenti cartacei

Le informazioni personali su supporto cartaceo devono essere custodite in modo da evitare la loro possibile diffusione, anche casuale, a persone non autorizzate.

I documenti cartacei contenenti dati personali non devono essere lasciati incustoditi presso attrezzature condivise (stampanti, fotocopiatrici…) o abbandonati sulla propria scrivania ma devono essere conservati in armadi chiusi a chiave all'interno di spazi sicuri. La chiave per l'apertura dell'armadio può essere condivisa solo con persone o funzioni con lo stesso livello di autorizzazione all'accesso ai dati.

Lasciare la scrivania pulita al termine della giornata di lavoro, riponendo tutti i documenti cartacei all'interno degli appositi spazi, è il primo passo per ridurre il rischio di rischio di perdita, di sottrazione di dati personali o di loro diffusione a persone non autorizzate (ad esempio personale della ditta di pulizie).

Al personale autorizzato al trattamento è richiesto di attenersi a questi comportamenti.

9.2 Trasmissione e riproduzione di documenti cartacei

La stampa o la fotocopia di un documento che contiene informazioni personali richiede l'adozione delle cautele appresso richiamate.

Le apparecchiature con funzioni di stampa e di copia sono solitamente situate in spazi aperti e, nel caso in cui il luogo di lavoro sia condiviso con altri soggetti, sono facilmente accessibili da parte di terzi non autorizzati. Per questo motivo, è richiesto di non lasciare incustoditi presso la stampante documenti contenenti dati personali di individui e di ritirare la stampa appena disponibile; allo stesso modo, è richiesto di essere presenti mentre la macchina sta effettuando la copia richiesta.

Pagine eventualmente scartate perché mal stampate o inceppate devono essere ritirate e distrutte secondo quanto indicato successivamente nel presente documento.

9.3 Smaltimento di documenti cartacei

Lo smaltimento e l'eliminazione dei documenti cartacei è un tema da valutare opportunamente per i rischi connessi a trattamenti effettuabili da personale non autorizzato.

Trascorso un determinato arco temporale, la conservazione di alcuni documenti non è più richiesta per vari motivi: le informazioni sono diventate obsolete, hanno esaurito il loro ciclo di vita o hanno semplicemente esaurito la funzione per la quale erano state prodotte e conservate.

La loro conservazione è sconsigliata, non solo perché comporta costi importanti collegati alla dimensione degli spazi, alla necessità di protezione degli stessi da rischi di incendio, da perdite d'acqua o da accessi indesiderati ma anche perché, in alcuni casi, l'eliminazione dei documenti che contengono dati personali è richiesta per legge.

Infatti, i dati personali in possesso di CNIT devono essere cancellati secondo i termini comunicati agli interessati al momento della raccolta dei loro dati e cioè allo scadere del termine di conservazione indicato per ciascuna finalità di trattamento; per ottemperare a tale obbligo normativo, la cancellazione deve perciò estendersi a ogni documento cartaceo che li contenga.

Analogamente a quanto previsto per i documenti elettronici conservati sul disco fisso della postazione di lavoro assegnata, ogni Utente è responsabile del controllo e della custodia dei documenti cartacei da lui stampati o fotocopiati nonché della loro eliminazione quando questi non sono più necessari per lo svolgimento delle proprie mansioni.

La documentazione cartacea non più necessaria deve essere eliminata utilizzando le apposite macchine distruggi documenti: ove queste non siano disponibili, la distruzione dei documenti deve avvenire con modalità tali da non permettere a un soggetto terzo di ricostruirne il contenuto.

10. Posta elettronica

Il servizio di posta elettronica è messo a disposizione degli Utenti abilitati come supporto per le attività svolte per conto di CNIT.

La posta elettronica è uno strumento di lavoro a supporto della comunicazione e dell'operatività interna. Gli Utenti assegnatari di indirizzi di posta elettronica sono responsabili del loro corretto utilizzo.

CNIT utilizza:

- caselle di posta elettronica ad uso individuale ed esclusivo dell'assegnatario, con userid nominativa ovvero non nominativa;
- indirizzi email di tipo personale (es: nome.cognome@cnit.it), assegnati ai singoli dipendenti;
- mailing list istituzionali, utilizzate per la distribuzione di comunicazioni a gruppi di destinatari individuati sulla base di criteri organizzativi o funzionali, quali, a titolo esemplificativo, l'appartenenza agli organi del Consorzio, alle Unità di Ricerca, a progetti o gruppi di lavoro, nonché l'adesione o l'interesse verso specifiche iniziative, eventi o altre attività istituzionali. La gestione delle mailing list e dei relativi iscritti è effettuata dalle strutture competenti in funzione delle esigenze organizzative e operative del CNIT.

L'Utente non deve utilizzare il servizio di posta elettronica e l'indirizzo e-mail di CNIT per:

- trasmettere o diffondere contenuti che siano illeciti, dannosi, minatori, abusivi, molesti, diffamatori e/o calunniosi, volgari, osceni, lesivi della privacy altrui, razzisti, classisti o comunque reprensibili;
- arrecare danno, in qualsivoglia modo, a minori di età;
- falsificare la propria identità o mentire circa il proprio rapporto con altri soggetti;
- creare intestazioni o in altro modo manipolare segni distintivi o indicazioni, al fine di contraffare l'origine di un contenuto trasmesso o diffuso tramite il servizio di posta elettronica;
- trasmettere o diffondere un contenuto che non abbia il diritto di trasmettere o diffondere in forza di una previsione di legge, di contratto ovvero in forza di un rapporto fiduciario (per esempio informazioni riservate, informazioni confidenziali apprese in forza di un rapporto di lavoro o protette da un patto di riservatezza);
- trasmettere o diffondere un contenuto che comporti la violazione di brevetti, marchi, segreti, diritti di autore o altri diritti di proprietà industriale e/o intellettuale di CNIT; dei suoi partner o di terzi soggetti;
- trasmettere o diffondere pubblicità, materiale promozionale, "junk mail", "spam", catene, piramidi, o qualsiasi altra forma di sollecitazione non autorizzate o non richieste;
- perseguitare o in altro modo molestare terzi soggetti;

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche. Se si dovessero ricevere messaggi di tale tipo, è opportuno darne comunicazione immediata al personale del Servizio Informativo per le eventuali azioni del caso; si raccomanda di non aprire per nessun motivo gli allegati a questo tipo di messaggio né di cliccare su eventuali link.

Particolare attenzione deve essere prestata dall'Utente ai cosiddetti messaggi di phishing o di social engineering, che spesso hanno l'obiettivo di sottrarre le credenziali utente per poi utilizzarle a fini criminali. Di solito questi messaggi sembrano provenire da fonti attendibili o note che chiedono di aprire un link o un allegato; anche se in alcuni casi questi messaggi presentano errori di ortografia, marchi contraffatti o generalità del mittente incomplete, gli autori di questi tentativi sono a volte in grado di confezionare messaggi molto verosimili e privi di errori. Ricordiamo che l'utilizzo di una credenziale di accesso deve essere sempre un'azione decisa dall'Utente; la richiesta di inserire in una maschera le proprie credenziali o di aprire un link è molto probabilmente indice di un tentativo malevolo (es. furto di credenziali, installazione di malware) ed è bene dunque cancellare immediatamente questi messaggi, senza aprire link o allegati. In caso di dubbio, l'Utente deve immediatamente segnalare alla Funzione IT la ricezione di questo tipo di messaggi.

La casella di posta deve essere mantenuta in ordine, scaricando i documenti di interesse di CNIT nelle apposite cartelle di reti e cancellando documenti inutili, con l'obiettivo di contenere le dimensioni della casella e di conservare dati personali e documenti in un unico luogo, dove sia più facile proteggerli adeguatamente e cancellarli nel momento in cui non siano più necessari.

È obbligatorio controllare gli allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

10.1 Periodi di assenza e inoltro automatico

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati da parte dell'A.d.S, nel rispetto del principio di necessità e di proporzionalità in caso di assenze pianificate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella, o malattia), il sistema può essere impostato con inoltro automatico dei messaggi verso un'altra casella di posta e contestuale notifica dell'inoltro al mittente. In caso di assenze programmate la funzionalità deve essere attivata dall'Utente; in caso di assenza non programmata (ad es. per malattia) o in casi del tutto eccezionali e motivati (es. scadenze impellenti), su richiesta della Direzione, sarà attivata dalla Funzione IT tramite accesso centralizzato la funzionalità per la quale al mittente sarà inviata un'e-mail automatica di risposta dal sistema, in cui sarà dichiarata l'assenza della risorsa destinataria e sarà fornito un contatto alternativo cui potersi rivolgere, senza la necessità di accedere direttamente alla casella di posta elettronica dell'Utente.

Al momento della cessazione del rapporto tra l'Utente e le Società, la Funzione IT, a seguito di apposita comunicazione della Direzione, provvederà alla cancellazione della casella di posta elettronica e del suo contenuto.

10.2 Tempi di conservazione dei log MTA e accesso ai log da parte dell'A.d.S. interno

La piattaforma in uso per il sistema di posta elettronica aziendale conserva attualmente i log MTA (Mail Transfer Agent) del sistema di posta elettronica per un periodo massimo di 21 giorni, come indicato dal Garante Italiano.

L'A.d.S. interno accederà ai log di sistema relativi agli Indirizzi e-mail esclusivamente in caso di necessità stringente e per esigenze legate esclusivamente alla gestione del servizio di posta elettronica; nel caso ciò avvenisse, l'A.d.S. interno manterrà riservate le informazioni di cui verrà a conoscenza durante l'accesso, fatta eccezione per quanto previsto e richiesto dalla legge.

11. Utilizzo dell'account Microsoft 365

L'account Microsoft è personale e assegnato a taluni Utenti tramite Userid e password.

L'account può essere utilizzato su tutte le risorse fisse e portatili assegnate da CNIT e sotto il controllo della Funzione IT.

11.1 Uso di Microsoft Exchange

Nell'ambito delle applicazioni informatiche in uso all'interno di CNIT è inserita anche la piattaforma Microsoft Exchange (in aggiunta al sistema di posta elettronica istituzionale che rimane comunque lo strumento prioritario). Questa conserva attualmente i log MTA per un periodo minimo di 90 giorni che non può essere ulteriormente ridotto[1].

Qualora il gestore di tale piattaforma fornisse nel futuro la possibilità di ridurre il periodo di conservazione dei suddetti log, in funzione delle opzioni che il gestore metterà a disposizione della clientela, CNIT modificherà la configurazione del servizio scegliendo la tempistica più vicina al termine massimo di conservazione, che non dovrebbe superare i 21 giorni.

Anche per tale piattaforma, l'A.d.S. interno accederà ai log di sistema relativi agli Indirizzi e-mail esclusivamente in caso di necessità stringente e per esigenze legate esclusivamente alla gestione del servizio di posta elettronica; nel caso ciò avvenisse, l'A.d.S. interno manterrà riservate le informazioni di cui verrà a conoscenza durante l'accesso, fatta eccezione per quanto previsto e richiesto dalla legge.

11.2 Uso di Microsoft Teams o di altri strumenti di video-conferenza

Nell'ambito delle applicazioni informatiche in uso all'interno di CNIT sono inserite le piattaforme Micorosft Teams, Zoom Workplacee e Goto Meeting, che permettono l'esecuzione di chiamate e videoconferenze. Tali piattaforme sono gestite dall'A.d.S. interno

Le suddette piattaforme si prestano ad attività di controllo del traffico e delle attività svolte, controllo che CNIT non ha attivato per lasciare all'Utente la massima libertà nell'organizzazione del lavoro.

Le stesse piattaforme emettono periodicamente report circa l'utilizzo della piattaforma da parte degli Utenti. Questi report hanno un carattere informativo e non sono inviati a CNIT, che non utilizza dunque tali informazioni per analisi sulle attività degli Utenti a cui è stata assegnata una Utenza operativa.

Le impostazioni del sistema di video-conferenza a disposizione di CNIT sono impostate di default dalla Funzione IT e non consentono agli esterni di entrare nelle riunioni telematiche senza l'autorizzazione dell'organizzatore o di membri autenticati di CNIT. Queste misure di sicurezza possono essere rimosse dal singolo Utente in fase di accesso all'evento o alla riunione.

12. Uso dei Social

12.1 Canali e profili social di CNIT

Le strategie di comunicazione effettuate mediante i canali e i profili social di CNIT devono essere concordate preventivamente con la Direzione; l'Utente autorizzato opera su canali e piattaforme social di CNIT mediante apposito account univoco in modo che sia possibile risalire a chi ha caricato i contenuti.

12.2 Profili social personali dei dipendenti: contenuti riferiti all'ambito lavorativo

Qualsiasi commento o post pubblicato dai dipendenti o consulenti di CNIT sui propri profili social personali, se riguarda l'ambito lavorativo, dovrebbe essere fatto con senso di responsabilità e rispetto nei confronti di CNIT, dei suoi partner e, in genere, del personale che a vario titolo partecipa alle varie attività. Fermo restando il diritto di ciascuno alla libera manifestazione del proprio pensiero, quando si esprimono opinioni personali in merito ad argomenti collegati all'attività lavorativa è sempre bene precisarlo (non è infatti detto che le opinioni espresse rispecchino la posizione del datore del lavoro).

La divulgazione da parte di dipendenti e collaboratori, attraverso i propri profili social personali, di informazioni su iniziative, decisioni, progetti e documenti di CNIT non ancora resi pubblici o non destinati a essere resi pubblici, è vietata.

[1] Il termine massino di conservazione di tali log indicato dal Garante Italiano è di 21 giorni, salvo necessità specifiche e motivate dell'ente, che devono essere formalizzate e approvate dall'INL. CNIT non ha alcuna necessità di conservare questi log per un tempo superiore ai 21 giorni ma non ha alcuna possibilità di ottenere dal fornitore del servizio una riduzione dei termini minimi.

È inoltre vietato raccogliere fotografie, file audio o registrazioni filmate nell'ambiente di lavoro, trasmetterle via chat a terze persone o diffonderle in rete.

CNIT si riserva il diritto di tutelare nelle sedi opportune il proprio onore e la propria reputazione qualora li ritenga pregiudicati da contenuti a lei riferiti ed espressi in modo volgare, offensivo e in contrasto con il limite della continenza da parte di un dipendente.

13. Navigazione in Internet

13.1 Regole generali

È esclusa la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa; in ogni caso i dipendenti devono astenersi dal visitare siti di puro intrattenimento o di svago.

Dalle postazioni di lavoro assegnate, è vietato:

- effettuare registrazioni e/o navigare in siti non attinenti allo svolgimento delle mansioni assegnate (quali a titolo esemplificativo siti idonei a rivelare preferenze sessuali, di giochi a premi o di aste);
- partecipare a forum; utilizzare chat line, bacheche elettroniche e registrazioni in guest book, anche utilizzando pseudonimi (o nicknames);
- scaricare file audio e/o video;
- effettuare il download di software gratuiti (freeware) e shareware da siti Internet;
- utilizzare tool/SW gratuiti disponibili in rete, se non autorizzati, per la redazione di documenti di lavoro o per l'analisi di dati e informazioni di CNIT;
- inserire in rete e/o memorizzare materiale di dubbio contenuto. A titolo esemplificativo e non esaustivo: documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, opinione e appartenenza sindacale e/o politica, materiale che favorisca attività illegali, materiale erotico o per soli adulti;
- utilizzare collegamenti Internet con meccanismi o apparati diversi dalla rete aziendale;
- effettuare qualsiasi tipo di attività volta a raggirare o compromettere i meccanismi di protezione dei sistemi informatici;
- sfruttare qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinsechi ai programmi e/o ai sistemi al fine di commettere azioni illecite o non autorizzate;
- utilizzare piattaforme di social media (Facebook, Twitter, YouTube, Instagram, etc.), Peer to Peer (P2P), file sharing, podcasting, webcasting o similari a meno che il loro utilizzo sia connesso all'attività lavorativa svolta;
- utilizzare sistemi di messaggistica istantanea quali Microsoft Messenger, Yahoo Messenger, Gmail chat etc. con la sola esclusione degli strumenti aziendalmente riconosciuti e autorizzati;
- effettuare ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi casi direttamente autorizzati dalla Direzione.

13.2 Regole esterne alla rete

È fatto assoluto divieto di utilizzare connessioni non sicure e aperte (non protette da password) per il collegamento alla rete con i dispositivi assegnati, come ad esempio reti WiFi gratuite.

La connessione alla rete mediante l'utilizzo dello smartphone assegnato da CNIT è da considerarsi adeguata ai livelli di sicurezza richiesti, purché sia protetta da password per l'accesso (la cui complessità rispetti le regole previste dal presente documento) e non sia condivisa con altri dispositivi non autorizzati o non assegnati all'Utente.

La connessione alla rete mediante l'utilizzo di dispositivi di connessione appartenenti all'Utente (ad esempio nel caso di prestazione dell'attività lavorativa dalla propria abitazione) è da considerarsi adeguata ai livelli di sicurezza richiesti se rispetta le seguenti regole:

- per l'accesso alla rete WiFi e alla configurazione dispositivo di connessione è richiesta una password forte che rispetti i parametri richiesti dal presente documento;
- l'accesso alla rete mediante il dispositivo di connessione è limitato all'Utente e ai suoi conviventi;

- l’apparato di connessione è fisicamente situato in una zona inaccessibile a persone sconosciute o non conviventi con l’Utente.

14. Protezione antivirus

Il sistema Informativo e gli archivi sono protetti mediante sistemi di protezione antivirus costantemente aggiornati. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco ai Servizi IT del CNIT mediante virus o altro software dannoso.

L’Utente non deve in alcun modo impedire gli aggiornamenti automatici del sistema antivirus.

Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto alla Funzione IT, attenendosi alle istruzioni ricevute.

Ogni supporto informatico esterno contenente dati, prima di essere utilizzato, deve essere sottoposto a scansione dal programma antivirus. Nel caso sia rilevato un virus, il supporto dovrà essere prontamente messo a disposizione della Funzione IT.

15. Sistemi di controllo e modalità operative

CNIT ha la facoltà di effettuare controlli sui documenti contenuti nei propri Sistemi informativi anche attraverso l’impiego di specifici strumenti IT; i controlli hanno lo scopo di tutelare il patrimonio informatico di CNIT, di verificare la sicurezza dei sistemi informativi e il loro corretto utilizzo da parte degli Utenti.

In caso fossero riscontrate anomalie di comportamento da parte degli Utenti o un utilizzo delle Risorse Informatiche non in linea con le prescrizioni del presente Regolamento, la Funzione IT effettuerà controlli che, qualora se ne ravvisasse la necessità, si concluderanno con avvisi generalizzati diretti agli Utenti allo scopo di richiamare la necessità di attenersi scrupolosamente alle istruzioni impartite. Controlli a carattere individuale saranno avviati solo se gli avvisi di carattere generale emanati non abbiano prodotto i risultati attesi.

In nessun caso saranno attuati controlli prolungati, costanti o indiscriminati.

I dati personali relativi agli accessi alle risorse aziendali e al traffico telematico sono cancellati automaticamente e periodicamente, a meno dei casi in cui la loro conservazione sia necessaria per:

- particolari esigenze tecniche o di sicurezza;
- indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

L’accesso, per verifiche e audit, ai sistemi informatici di posta elettronica aziendale e alle postazioni di lavoro, potrà essere richiesto per motivate ragioni dalla Direzione. Le verifiche saranno effettuate secondo le modalità previste dalla normativa vigente e del CCNL applicato, nel rispetto delle prescrizioni vigenti sulla tutela della privacy.

16. Sanzioni

È fatto obbligo a tutti gli Utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento interno. Il mancato rispetto delle regole sopra ricordate, la loro violazione o eventuali illeciti potranno essere sanzionate nei termini previsti dal CCNL applicabile.

CNIT si riserva il diritto di rivolgersi all’autorità giudiziaria nel caso ritenesse di sere in presenza di illeciti di rilevanza penale.

17. Storia del documento e revisioni

Il presente documento è soggetto a revisione periodica; gli aggiornamenti sono pubblicati sul sito del CNIT www.cnit.it.

ALLEGATO 1

PRESCRIZIONI PER GLI UTENTI DEGLI STRUMENTI DI LAVORO E DEI SISTEMI IT DEL CNIT

Riservatezza, protezione dei dati e sicurezza delle informazioni

1. L'Utente deve mantenere la riservatezza sulle informazioni, sui processi interni e sui rapporti con i partner di CNIT e non deve diffondere senza autorizzazione informazioni aziendali riservate o dati personali degli interessati (cfr. § 4).
2. L'Utente autorizzato a svolgere trattamenti di dati personali per conto di CNIT deve conoscere, in relazione alle mansioni svolte e al livello di responsabilità assegnato, gli aspetti rilevanti della disciplina sulla protezione dei dati personali, i rischi che incombono sui dati e sui trattamenti, le misure disponibili per prevenire eventi dannosi e i comportamenti da adottare nelle operazioni quotidiane e nelle situazioni di emergenza (cfr. § 4.1).
3. Le operazioni di trattamento di dati personali devono essere effettuate conformemente alle istruzioni contenute nel Regolamento (cfr. § 4.2).
4. L'Utente deve rispettare le misure di sicurezza tecniche e organizzative adottate da CNIT e non deve tentare di superare o forzare tali misure (cfr. § 4.2).
5. L'Utente non deve divulgare a terzi informazioni relative alle misure di sicurezza applicate, incluse password, credenziali e altri codici di accesso, né informazioni relative alle procedure, agli strumenti e ai sistemi utilizzati per effettuare i trattamenti di dati (cfr. § 4.2).
6. L'Utente è tenuto al rispetto degli obblighi di fedeltà e riservatezza anche dopo la cessazione, per qualsiasi causa e motivo, del rapporto con CNIT (cfr. § 4.2).

Furto o smarrimento di dispositivi e supporti

7. In caso di furto o smarrimento di risorse informatiche aziendali assegnate o di dispositivi contenenti informazioni di CNIT o dati personali, l'Utente deve avvertire tempestivamente la Direzione, inviare all'indirizzo direzione@cnit.it una e-mail contenente una breve descrizione dell'accaduto, effettuare denuncia presso le autorità competenti e inviarne copia alla Direzione per l'archiviazione (cfr. § 4.3).
8. In caso di furto di supporti informatici contenenti informazioni proprietarie, quali chiavette USB o dischi esterni, l'Utente deve effettuare denuncia presso le autorità competenti e inviarne copia alla Direzione per l'archiviazione (cfr. § 4.3).
9. Le risorse informatiche assegnate all'Utente, in forma esclusiva o condivisa, devono essere utilizzate esclusivamente per scopi leciti connessi con l'attività lavorativa (cfr. § 4.3).

Utilizzo di strumenti di Intelligenza Artificiale generativa

10. Qualora contenuti generati mediante sistemi di intelligenza artificiale siano destinati alla diffusione o alla condivisione con terzi, l'Utente deve indicare, ove appropriato, che tali contenuti sono stati elaborati con il supporto di strumenti di intelligenza artificiale (cfr. § 4.4).
11. L'Utente è responsabile della verifica, del controllo e della validazione dei contenuti, delle informazioni e del codice generati mediante sistemi di intelligenza artificiale prima del loro utilizzo in documenti ufficiali, comunicazioni, processi decisionali o applicazioni software (cfr. § 4.4).
12. È vietato inserire nei sistemi di intelligenza artificiale pubblici o gratuiti dati personali, in particolare se appartenenti a categorie particolari, nonché informazioni riservate, confidenziali o comunque riconducibili all'organizzazione, compresi codice sorgente, configurazioni di sistema, credenziali, chiavi crittografiche, token di autenticazione e documentazione tecnica, salvo i casi espressamente autorizzati e nel rispetto della normativa vigente (cfr. § 4.4).

Credenziali di accesso e password

13. Le credenziali utente sono ad uso strettamente personale, devono essere utilizzate esclusivamente per ragioni di lavoro e adeguatamente custodite; è vietato comunicarle ad altre persone, al fine di evitare utilizzi non autorizzati dei Servizi IT da parte di terzi (cfr. §§ 6.3 e 6.3.1).
14. L'Utente non deve comunicare la propria password all'Amministratore di Sistema o ad altri soggetti, salvo particolari necessità previste dal Regolamento e su esplicita richiesta di supporto operativo; in tali casi, al termine dell'intervento deve effettuare immediatamente il reset della password (cfr. § 6.3).

15. È vietato memorizzare le credenziali di accesso sul dispositivo, ad esempio all'interno di file Word o Excel o nella cache del browser, o su supporti cartacei (cfr. § 6.3.1).
16. È vietato utilizzare credenziali assegnate ad altri utenti per accedere alla rete, ai sistemi o alle applicazioni (cfr. § 6.3.1).
17. La password iniziale deve essere obbligatoriamente modificata dall'Utente al primo accesso (cfr. § 7).
18. Non è consentito utilizzare la stessa password per accedere a più servizi o applicazioni o in associazione a più userid (cfr. § 7).
19. La password deve essere composta utilizzando lettere minuscole e maiuscole, numeri e caratteri speciali e deve avere una lunghezza minima di 8 caratteri; ove consentito dal sistema, è preferibile una lunghezza di almeno 12 caratteri (cfr. § 7).
20. La password non deve contenere elementi facilmente riconducibili all'Utente, quali nomi di componenti del nucleo familiare, animali di famiglia o date di nascita, e non deve coincidere con la userid (cfr. § 7).
21. La password deve essere diversa dalle cinque precedentemente utilizzate (cfr. § 7).
22. L'Utente deve mantenere riservata la propria password e modificarla immediatamente qualora sospetti che qualcuno possa averla individuata, anche se il relativo termine di validità non è ancora scaduto (cfr. § 7).

Archiviazione e gestione dei file

23. Le cartelle condivise devono essere utilizzate esclusivamente per informazioni strettamente professionali; nessun file non legato all'attività lavorativa può essere memorizzato, nemmeno temporaneamente, in tali unità (cfr. § 8.1).
24. L'Utente deve limitare la memorizzazione di dati personali negli archivi locali allo stretto necessario e a quanto motivato dalle mansioni svolte, privilegiando l'utilizzo delle cartelle condivise predisposte da CNIT per i documenti rilevanti per l'attività lavorativa (cfr. § 8.1).
25. L'Utente deve effettuare revisioni periodiche, almeno ogni tre mesi, degli archivi locali, cancellando i file obsoleti o non più utili per lo scopo per il quale sono stati creati (cfr. § 8.1).
26. L'Utente non deve trasmettere ai colleghi mediante posta elettronica file contenenti dati personali degli interessati; deve preferire l'invio del collegamento alla cartella condivisa ai colleghi autorizzati che necessitano di accedere ai dati (cfr. § 8.1).
27. Nessun file di carattere personale può essere memorizzato nello spazio disco della postazione di lavoro assegnata (cfr. § 8.1).
28. Non è consentito conservare in locale documenti con estensione file non riconosciuta dai sistemi di CNIT (cfr. § 8.1).
29. L'Utente è responsabile del salvataggio e del backup dei dati conservati sia negli archivi locali sia nelle cartelle condivise in rete (cfr. § 8.2).

Supporti di memorizzazione e supporti rimovibili

30. I supporti informatici contenenti o che abbiano contenuto dati personali possono essere riutilizzati esclusivamente previa cancellazione permanente del loro contenuto; la riformattazione veloce o la semplice cancellazione dei file non sono sufficienti (cfr. § 8.3).
31. I supporti digitali contenenti dati personali non destinati alla conservazione devono essere distrutti secondo le indicazioni della Funzione IT (cfr. § 8.3).
32. I supporti rimovibili contenenti dati personali o informazioni costituenti know-how di CNIT o dei suoi afferenti devono essere trattati con particolare cautela e custoditi in armadi chiusi, evitando che il loro contenuto possa essere sottratto, alterato, distrutto o recuperato successivamente alla cancellazione (cfr. § 8.9).
33. È vietato utilizzare supporti rimovibili personali non preventivamente autorizzati dalla Direzione (cfr. § 8.9).
34. L'Utente è responsabile della custodia dei supporti rimovibili e del relativo contenuto (cfr. § 8.9).

Personal computer e laptop

35. Non è consentito trasferire un personal computer da un assegnatario a un altro senza informare preventivamente la Funzione IT (cfr. § 8.4).
36. Il PC assegnato all'Utente deve essere utilizzato quale strumento di lavoro; l'utilizzo deve pertanto essere inerente all'attività lavorativa (cfr. § 8.6).

37. L'Utente deve custodire con diligenza il PC assegnato, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, adottando i provvedimenti necessari per evitare danni o sottrazioni (cfr. § 8.6).
38. È vietato utilizzare programmi diversi da quelli ufficialmente installati o autorizzati da CNIT ed è vietato installare autonomamente programmi (cfr. § 8.6).
39. Salvo preventiva espressa autorizzazione della Direzione e della Funzione IT, l'Utente non può modificare la configurazione hardware o software o le caratteristiche impostate sul PC, né installare dispositivi di memorizzazione, comunicazione o altri dispositivi (cfr. § 8.6).
40. L'Utente deve prestare la massima attenzione ai supporti di origine esterna e deve avvertire immediatamente la Funzione IT qualora rilevi virus o ne sospetti l'esistenza (cfr. § 8.6).
41. Il PC deve essere spento in caso di assenze prolungate dall'ufficio o in caso di inutilizzo (cfr. § 8.6).
42. L'Utente non deve modificare le funzioni e gli aggiornamenti di sicurezza gestiti dalla Funzione IT (cfr. § 8.6).

Smartphone, tablet e altri dispositivi mobili

43. L'Utente deve custodire con diligenza smartphone e tablet aziendali assegnati, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, adottando i provvedimenti necessari per evitare danni o sottrazioni (cfr. § 8.7).
44. Sugli smartphone e tablet aziendali devono essere scaricate esclusivamente applicazioni necessarie allo svolgimento e alla semplificazione dell'attività lavorativa (cfr. § 8.7).
45. È vietato modificare i dispositivi mobili mediante manipolazione software o installare applicazioni non appartenenti agli App Store dei produttori (cfr. § 8.7).
46. Le applicazioni di messaggistica devono essere utilizzate solo per necessità stringenti; è vietato utilizzarle per trasmettere file o archivi contenenti informazioni o dati personali gestiti da CNIT (cfr. § 8.7).
47. Il servizio di fonia mobile non deve essere utilizzato per trasmettere o diffondere contenuti illeciti, dannosi, minatori, abusivi, molesti, diffamatori, calunniosi, volgari, osceni, lesivi della privacy altrui, discriminatori o comunque reprensibili (cfr. § 8.7).
48. Il servizio di fonia mobile non deve essere utilizzato per falsificare la propria identità, contraffare l'origine dei contenuti, diffondere informazioni che l'Utente non abbia diritto di comunicare, violare diritti di proprietà industriale o intellettuale, diffondere comunicazioni promozionali non autorizzate o molestare soggetti terzi (cfr. § 8.7).
49. I dispositivi mobili aziendali non devono essere utilizzati in contesti nei quali persone non autorizzate possano entrare in contatto con informazioni di CNIT o dati personali trattati; in particolare, l'Utente deve prestare attenzione affinché altre persone non possano visualizzare, anche occasionalmente, il contenuto dello schermo (cfr. § 8.8).
50. I dispositivi mobili non devono essere lasciati incustoditi in luoghi pubblici (cfr. § 8.8).
51. L'utilizzo dei dispositivi mobili aziendali non deve essere consentito a persone non autorizzate ad accedere alle informazioni aziendali (cfr. § 8.8).
52. L'accesso ai dispositivi mobili deve avvenire mediante autenticazione con credenziali, codici o sistemi biometrici secondo gli standard supportati dallo strumento (cfr. § 8.8).

Documenti cartacei

53. Le informazioni personali su supporto cartaceo devono essere custodite in modo da evitarne la diffusione, anche accidentale, a persone non autorizzate (cfr. § 9.1).
54. I documenti cartacei contenenti dati personali non devono essere lasciati incustoditi presso stampanti, fotocopiatrici o altre attrezzature condivise né abbandonati sulla scrivania, ma devono essere conservati in armadi chiusi a chiave all'interno di spazi sicuri (cfr. § 9.1).
55. Le chiavi degli armadi contenenti documenti con dati personali possono essere condivise esclusivamente con persone o funzioni aventi il medesimo livello di autorizzazione all'accesso ai dati (cfr. § 9.1).
56. In caso di stampa di documenti contenenti dati personali, l'Utente deve ritirare la stampa appena disponibile e non deve lasciare i documenti incustoditi presso la stampante (cfr. § 9.2).
57. In caso di fotocopia di documenti contenenti dati personali, l'Utente deve essere presente durante l'esecuzione della copia (cfr. § 9.2).

58. Le pagine scartate perché mal stampate o inceppate devono essere ritirate e distrutte con modalità idonee (cfr. § 9.2).
59. L'Utente è responsabile del controllo e della custodia dei documenti cartacei da lui stampati o fotocopiati e della loro eliminazione quando non siano più necessari per lo svolgimento delle proprie mansioni (cfr. § 9.3).
60. La documentazione cartacea non più necessaria deve essere eliminata mediante le apposite macchine distruggi-documenti o, qualora queste non siano disponibili, con modalità tali da impedire a terzi di ricostruirne il contenuto (cfr. § 9.3).

Posta elettronica

61. La posta elettronica di CNIT deve essere utilizzata esclusivamente come strumento di lavoro e per attività svolte per conto di CNIT (cfr. § 10).
62. L'Utente non deve utilizzare la posta elettronica di CNIT per trasmettere o diffondere contenuti illeciti, dannosi, minatori, abusivi, molesti, diffamatori, calunniosi, volgari, osceni, lesivi della privacy, discriminatori o comunque reprensibili (cfr. § 10).
63. L'Utente non deve utilizzare la posta elettronica per falsificare la propria identità o l'origine di contenuti, diffondere informazioni che non abbia diritto di comunicare, violare diritti di proprietà industriale o intellettuale, trasmettere pubblicità o comunicazioni non richieste o molestare terzi (cfr. § 10).
64. È vietato utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa, compresi l'invio o ricezione di materiale multimediale non lavorativo, messaggi personali, partecipazione a dibattiti, aste online, concorsi, forum, mailing list o catene telematiche (cfr. § 10).
65. Qualora riceva messaggi appartenenti a catene telematiche, l'Utente deve evitare di aprire allegati o collegamenti (cfr. § 10).
66. L'Utente deve prestare particolare attenzione ai messaggi di phishing o social engineering e non deve inserire le proprie credenziali in maschere né aprire collegamenti o allegati contenuti in messaggi sospetti; in caso di dubbio sulla natura di un messaggio, deve segnalarlo immediatamente alla Funzione IT (cfr. § 10).
67. La casella di posta elettronica deve essere mantenuta in ordine, salvando i documenti di interesse di CNIT nelle apposite cartelle di rete e cancellando i documenti inutili (cfr. § 10).
68. L'Utente deve controllare gli allegati di posta elettronica prima del loro utilizzo e non deve scaricare file eseguibili o documenti da siti Web o FTP non conosciuti (cfr. § 10).
69. In caso di assenze programmate, l'Utente deve attivare le funzionalità previste per garantire la continuità del servizio di posta elettronica secondo quanto stabilito dal Regolamento (cfr. § 10.1).

Account Microsoft 365

70. L'account Microsoft 365 è personale e deve essere utilizzato esclusivamente sulle risorse fisse e portatili assegnate da CNIT e poste sotto il controllo della Funzione IT (cfr. § 11).

Social media e contenuti relativi all'attività lavorativa

71. Le strategie di comunicazione effettuate mediante i canali e i profili social di CNIT devono essere preventivamente concordate con la Direzione e l'Utente autorizzato deve operare mediante l'apposito account assegnato (cfr. § 12.1).
72. I commenti o post pubblicati sui profili social personali e riferiti all'ambito lavorativo dovrebbero essere effettuati con senso di responsabilità e rispetto nei confronti di CNIT, dei suoi partner e del personale coinvolto nelle relative attività (cfr. § 12.2).
73. Quando esprime sui propri profili social opinioni personali su argomenti collegati all'attività lavorativa, l'Utente dovrebbe precisare che si tratta di opinioni personali e non della posizione di CNIT (cfr. § 12.2).
74. È vietato divulgare attraverso profili social personali informazioni su iniziative, decisioni, progetti e documenti di CNIT non ancora resi pubblici o non destinati a essere resi pubblici (cfr. § 12.2).
75. È vietato raccogliere fotografie, file audio o registrazioni filmate nell'ambiente di lavoro e trasmetterli tramite chat a terzi o diffonderli in rete (cfr. § 12.2).

Navigazione Internet e connessioni di rete

76. La navigazione Internet deve essere effettuata esclusivamente per motivi legati all'attività lavorativa; è pertanto vietato visitare siti di puro intrattenimento o svago, effettuare registrazioni o navigare in siti non attinenti allo svolgimento delle mansioni assegnate (cfr. § 13.1).
77. È vietato partecipare a forum, utilizzare chat line o bacheche elettroniche ed effettuare registrazioni in guest book, anche mediante pseudonimi o nickname (cfr. § 13.1).
78. È vietato scaricare file audio o video nonché software freeware o shareware da siti Internet (cfr. § 13.1).
79. È vietato utilizzare strumenti o software gratuiti disponibili in rete, se non autorizzati, per la redazione di documenti di lavoro o l'analisi di dati e informazioni di CNIT (cfr. § 13.1).
80. È vietato inserire in rete o memorizzare materiale di dubbio contenuto, compreso materiale oltraggioso, discriminatorio, relativo ad attività illegali, erotico o destinato esclusivamente a un pubblico adulto (cfr. § 13.1).
81. È vietato utilizzare collegamenti Internet con meccanismi o apparati diversi dalla rete aziendale, salvo quanto espressamente consentito dal Regolamento per il lavoro svolto all'esterno della rete CNIT (cfr. §§ 13.1 e 13.2).
82. È vietata qualsiasi attività diretta a raggirare o compromettere i meccanismi di protezione dei sistemi informatici, nonché sfruttare vulnerabilità derivanti da difetti di configurazione, dei programmi o dei sistemi allo scopo di compiere azioni illecite o non autorizzate (cfr. § 13.1).
83. Le piattaforme social, i sistemi Peer-to-Peer, file sharing, podcasting, webcasting o strumenti analoghi possono essere utilizzati esclusivamente quando il loro utilizzo sia connesso all'attività lavorativa (cfr. § 13.1).
84. È vietato utilizzare sistemi di messaggistica istantanea diversi dagli strumenti riconosciuti e autorizzati da CNIT (cfr. § 13.1).
85. È vietato effettuare transazioni finanziarie, comprese operazioni di remote banking e acquisti online, salvo i casi direttamente autorizzati dalla Direzione (cfr. § 13.1).
86. È vietato utilizzare connessioni non sicure e aperte, non protette da password, quali reti Wi-Fi gratuite, per collegare alla rete i dispositivi assegnati (cfr. § 13.2).
87. La connessione mediante smartphone assegnato da CNIT deve essere protetta da password conforme alle prescrizioni del Regolamento e non deve essere condivisa con dispositivi non autorizzati o non assegnati all'Utente (cfr. § 13.2).
88. Quando utilizza un proprio dispositivo di connessione per svolgere attività lavorativa, l'Utente deve proteggere mediante password forte sia l'accesso alla rete Wi-Fi sia la configurazione del dispositivo, limitare l'accesso alla rete a sé stesso e ai propri conviventi e collocare fisicamente l'apparato in una zona non accessibile a persone sconosciute o non conviventi (cfr. § 13.2).

Protezione antivirus e gestione degli incidenti

89. L'Utente non deve impedire in alcun modo gli aggiornamenti automatici del sistema antivirus (cfr. § 14).
90. Qualora il software antivirus rilevi la presenza di un virus, l'Utente deve sospendere immediatamente ogni elaborazione in corso senza spegnere il computer, segnalare prontamente l'accaduto alla Funzione IT e attenersi alle istruzioni ricevute (cfr. § 14).
91. Ogni supporto informatico esterno contenente dati deve essere sottoposto a scansione antivirus prima dell'utilizzo (cfr. § 14).
92. Qualora su un supporto informatico esterno sia rilevato un virus, l'Utente deve mettere prontamente il supporto a disposizione della Funzione IT (cfr. § 14).

Osservanza del Regolamento

93. Tutti gli Utenti sono tenuti a osservare le disposizioni contenute nel Regolamento; il mancato rispetto delle prescrizioni, la loro violazione o eventuali illeciti possono essere sanzionati nei termini previsti dal CCNL applicabile, ferme restando le ulteriori conseguenze previste dalla legge (cfr. §§ 4.2 e 16).