ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI
MILANO

# Disciplinare di utilizzo delle risorse informatiche

Regolamenta l'accesso e l'utilizzo delle risorse informatiche del Titolare con l'obiettivo di garantire la riservatezza, l'integrità e la disponibilità dei dati trattati dalle persone autorizzate al trattamento dei dati personali

Versione Aggiornata con integrazioni approvate con delibera di Consiglio del 29 settembre 2025
Versione Aggiornata al 28 dicembre 2021

**SOMMARIO**

# 1.INTRODUZIONE

## 1.1. GLOSSARIO

- Titolare: persona fisica, giuridica, ente o associazione che decide in merito alle finalità del trattamento e gli strumenti oltre che alla sicurezza. Ove nel documento si fa riferimento a Organizzazione si intende il Titolare.
- Responsabile: persona fisica, giuridica, società, ente o associazione che tratta i dati per conto del Titolare.
- Utenti o Autorizzati: dipendente o collaboratore (anche esterno) dell'Organizzazione in possesso di specifiche credenziali di autenticazione il quale è autorizzato ad effettuare materialmente le operazioni di trattamento dei dati personali.
- Amministratore di sistema: figura, fisica o giuridica, che gestisce il Sistema Informativo del Titolare. Sotto tale definizione ricadono anche amministratori di sottoinsiemi come ad esempio: le singole applicazioni gestionali, i database, la rete locale e gli apparati di sicurezza.
- Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, registrazione, organizzazione, conservazione, consultazione, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione di dati, anche se non registrati in una banca dati.
- Contratto: accordo che fonda un rapporto giuridico tra due parti come, ad esempio, un contratto di lavoro, un contratto di consulenza professionale, un contratto di fornitura, ecc.
- Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile (il cosiddetto "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 on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- Dati identificativi: i dati personali che permettono l'identificazione diretta dell'Interessato.
- Dati particolari: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose o filosofiche, le opinioni politiche, l'appartenenza sindacale, nonché i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a o) e da r) a u) del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- Riservatezza: proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi che non sono autorizzati.
- Integrità: proprietà relativa alla salvaguardia dell'accuratezza e della completezza dell'informazione.
- Disponibilità: facoltà di un sistema informatico o di un'informazione di essere accessibile e utilizzabile su richiesta di un Autorizzato.
- Sicurezza delle informazioni: disciplina atta a garantire la riservatezza, l'integrità e la disponibilità delle informazioni al livello definito; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.
- Business Continuity (continuità operativa): l'insieme di attività, processi, ruoli e responsabilità che garantiscono la sopravvivenza del business/attività/servizi anche in situazioni impreviste, di disastro, perdita di disponibilità prolungata o fattori critici particolarmente gravi; l'obiettivo è garantire la disponibilità delle attività critiche in tutte le situazioni, sebbene a regimi ridotti o con lentezze nel caso di disastri gravi.
- Disaster Recovery: la componente tecnologia e procedurale della Business Continuity. Essa ha

carattere prevalentemente informatico e può essere quindi definita come l'insieme di tecnologie, strumenti di recupero, siti, postazioni, server, ecc. volti ad assicurare la continuità dell'infrastruttura informatica anche in caso di situazioni di disastro; è parte della strategia e dei piani di dettaglio della Business Continuity.

- CED: spesso indicato anche come Data Center, si intende una struttura fisica, normalmente un edificio o un locale compartimentato - unitamente a tutti gli impianti elettrici, di condizionamento, di attestazioni di rete, di cablaggi, ecc. e a sistemi di sicurezza fisica e logica - progettato e allestito per ospitare e gestire un numero elevato di apparecchiature e infrastrutture informatiche, e i dati ivi contenuti, allo scopo di garantirne la sicurezza fisica e gestionale.
- Cloud: insieme di tecnologie che permettono a un provider di fornire, in forma di servizio, l'elaborazione, l'archiviazione e la memorizzazione dei dati. Ciò viene solitamente realizzato utilizzando una connessione di rete e risorse hardware/software distribuite e virtualizzate.
- Log: la registrazione cronologica delle operazioni eseguite su di un sistema informatico, e quindi su archivi, per finalità quali ad esempio: controllo e verifica degli accessi (access log), registro e tracciatura dei cambiamenti che le transazioni introducono in un Database (log di transazioni o log di base dati), analisi delle segnalazioni di errore (error log), produzione di statistiche di esercizio.
- User-id o nome utente o codice utente o login-id: definisce il nome con il quale l'Utente viene riconosciuto da un computer, da un programma, da un server o da un sistema informatico in genere. In altre parole, esso è un identificativo che, unitamente alla password, costituisce le credenziali per poter accedere al sistema a cui esse sono correlate.
- Dominio.it: si intende il dominio internet del Titolare denominato odcec.mi.it.
- Area o Reparto o Funzione o Ufficio: identifica un'unità del Titolare preposta alla gestione di un particolare ambito organizzativo. Ciascuna Area (e/o Reparto e/o Funzione e/o Ufficio) ha propri compiti e responsabilità e svolge specifiche operazioni; tutti, però, sono collegati e coordinati tra loro e insieme operano per il conseguimento dei fini del Titolare.
- Sistema Informativo: insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Organizzazione.
- Disciplinare: il presente documento.

## 1.2. OGGETTO E FINALITÀ

Il presente Disciplinare è redatto:

- in relazione alla Legge 20-05-1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo n. 679/16 "General Data Protection Regulation" (d'ora in avanti "Reg. n. 679/16" o "GDPR");
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10- 03-2007;
- alla luce dell'art. 4, Stat. Lav. in tema di controlli attuabili da parte del datore di lavoro.

La finalità è quella di promuovere in tutti gli Autorizzati una corretta "cultura informatica" affinché l'utilizzo degli strumenti informatici e telematici forniti dal Titolare sia conforme alle finalità per le quali sono stati messi a disposizione degli Autorizzati stessi e nel pieno rispetto della legge. Si vuole fornire a tutti gli

Autorizzati le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto allaloro successiva correzione.

## 1.3. PRINCIPI GENERALI E DI RISERVATEZZA

1. I principi che sono a fondamento del presente Disciplinare sono gli stessi espressi nel GDPR, e, precisamente:
   1.1. il principio di **necessità,** secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di Dati personali e di Dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del GDPR);
   1.2. i trattamenti devono essere effettuati **per finalità determinate, esplicite e legittime** (art. 5 comma 1 lett. b) e c) GDPR), osservando il principio di **pertinenza e non eccedenza**. Il Titolare deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza";
   1.3. i principi di **correttezza e trasparenza**, secondo i quali il Titolare è tenuto a rendere note agli Interessati le informazioni principali relative al Trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 5 e 12 GDPR).
2. È riconosciuto al Titolare il potere di svolgere attività di monitoraggio, che nella fattispecie saranno svolte dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.
3. L'Autorizzato si attiene alle seguenti regole di trattamento.
   3.1. È vietato comunicare a soggetti non specificatamente autorizzati dal Titolare i Dati personali dei quali l'Autorizzato viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Organizzazione. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio responsabile di Area.
   3.2. È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e di quant'altro l'Autorizzato viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Organizzazione
   3.3. È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere Dati personali e/o informazioni quando l'Autorizzato si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, armadi, ecc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento.
   3.4. Per le riunioni e gli incontri con clienti, fornitori, consulenti e collaboratori dell'Organizzazione è preferibile utilizzare le eventuali zone e sale dedicate alle riunioni.

## 1.4. TUTELA DEL LAVORATORE

1. Alla luce dell'art. 4, comma 2, L. n. 300/1970, gli strumenti tecnologici in uso ai dipendenti dell'Organizzazione rientrano nel novero degli "strumenti utilizzati per rendere la prestazione lavorativa", tanto da esulare dal campo di applicazione dell'art. 4, comma 1, L. n. 300/1970 e dal rispetto del requisito teleologico e procedurale ivi previsto.
2. È garantito al singolo dipendente dell'Organizzazione in qualsiasi momento l'esercizio dei diritti dell'Interessato di cui agli artt. 15-16-17-18-20-21-22-77 del Reg. n. 679/16 scrivendo al Titolare al seguente indirizzo: helpdesk@odcec.mi.it

## 1.5. CAMPO DI APPLICAZIONE

Il presente Disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori del Titolare, anche esterni, a prescindere dal rapporto contrattuale intrattenuto.

## 1.6. CLASSIFICAZIONE DEL DOCUMENTO

Il presente Disciplinare di sicurezza è classificato come documento riservato e per solo uso interno: pertanto è vietato diffondere il presente documento al di fuori dell'ambito operativo dell'Organizzazione.

## 1.7. REVISIONE ED AGGIORNAMENTO

Il Titolare, che ha disposto il presente Disciplinare, ha l'incarico di procedere al suo riesame e alla verifica delle politiche di sicurezza complessive in seguito al verificarsi di:

- incidenti di sicurezza;
- variazioni tecnologiche significative e modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli standard di sicurezza desiderati;
- aggiornamenti delle prescrizioni minime di sicurezza richieste dalla normativa vigente;
- rilevazioni risultanti delle attività di audit.

In ogni caso, il riesame del presente documento e la verifica delle politiche di sicurezza sono svolti almeno con cadenza annuale da parte dell'Amministratore di Sistema.

# 2. REGOLE PER L'AUTORIZZATO

## 2.1. ACCESSO ALLE RISORSE INFORMATICHE

1. L'accesso alle risorse informatiche è consentito esclusivamente agli Autorizzati come definiti nel Glossario del presente Disciplinare.
2. Ogni risorsa informatica è affidata ad un Autorizzato che è responsabile della gestione e dell'utilizzo appropriato della risorsa stessa.
3. L'Autorizzato utilizza le risorse informatiche e riceve/inoltra comunicazioni sempre e solo nell'interesse del Titolare: è vietato l'uso per fini personali.
4. Il Titolare si riserva il diritto ad accedere alle risorse informatiche per compiti di gestione, controllo e/o aggiornamenti e per garantire la sicurezza del sistema e della rete nel rispetto del presente Disciplinare e della normativa vigente.

## 2.2. CLASSIFICAZIONE DELLE UTENZE

Sono definite tre tipologie distinte di utenze del Sistema Informativo:

- account funzionali: account attribuiti ad una struttura organicamente istituita (ad esempio, un'Area) e mai ad una persona fisica;
- account di servizio: account attribuiti a specifiche funzioni del Sistema Informativo e mai ad una persona fisica (ad esempio, per l'esecuzione automatica di applicazioni o parti di applicazioni);
- account personali: account attribuiti ad una persona fisica che ne è titolare e pienamente responsabile; tali account non sono cedibili. Sono assegnati agli Autorizzati che a vario titolo debbano utilizzare il Sistema Informativo. L'ufficio del personale dell'Organizzazione, ogni qualvolta si renda necessaria la creazione di una nuova user-id, ha l'incarico di: attestare l'identità dei soggetti esterni, dichiarare il loro rapporto con il Titolare, indicare la durata, o meglio la scadenza, dell'account.

Gli account funzionali e di servizio, al momento della creazione, sono attribuiti ad una o più persone fisiche identificate, e nominate con atto scritto, considerati responsabili per l'impiego di tali account.

## 2.3. POLITICHE DI GESTIONE DELLE IDENTITÀ DIGITALI

- Come predetto, ogni Autorizzato che accede al Sistema Informativo del Titolare è univocamente identificato attraverso l'assegnazione di un account personale (user-id e password). Al fine di identificare in maniera univoca ciascun utente del sistema, all'atto di richiesta di creazione dell'account, l'ufficio del personale dell'Organizzazione, tramite apposito modulo, fornisce tutti i dati richiesti all'Helpdesk.
- L'accesso alle risorse informative deve essere coerente con le mansioni lavorative assegnate. Le eccezioni a questa regola, quale ad esempio l'attribuzione di privilegi maggiori di quelli necessari, devono essere autorizzate e sottoscritte dal Titolare e documentate dall'Amministratore di Sistema.
- L'accesso alle risorse informatiche da parte di un Autorizzato deve essere concesso dall'Amministratore di Sistema solo dopo una formale richiesta da parte degli uffici competenti, a cui segue l'approvazione da parte del Titolare. L'autorizzazione per l'accesso al Sistema Informativo viene concessa a:
    - personale dipendente dell'Organizzazione, in relazione alle esigenze collegate allo svolgimento delle mansioni assegnate;
    - personale esterno all'Organizzazione, in relazione alle attività pianificate e programmate nei contratti di fornitura o derivanti dal rapporto giuridico che lo lega al Titolare.
- L'autorizzazione viene revocata quando non sussiste più la necessità di disporre delle risorse e/o delle informazioni (ad esempio, in caso di modifica delle mansioni, cessazione del servizio, termine o chiusura del Contratto). La responsabilità di segnalare tempestivamente la necessità di revoca dell'autorizzazione è in capo agli uffici preposti in relazione alla natura del rapporto se comunque non vi è una scadenza espressa nel modulo di creazione delle autorizzazioni.
- Le autorizzazioni per l'accesso ai dati e l'uso del Sistema Informativo sono concesse secondo procedure predefinite e formalizzate. I livelli di autorizzazione concessi devono, sotto la responsabilità dell'Amministratore di Sistema, essere riesaminati ed approvati almeno annualmente, al fine di verificare la sussistenza delle condizioni presenti al momento del loro iniziale rilascio.
- L'utilizzo di utenze privilegiate non imputabili ad un soggetto (root o amministratore di sistemi) è consentito solo per motivi di emergenza. Ai fini della tracciabilità delle operazioni, gli Utenti devono utilizzare la propria user-id personale, con le autorizzazioni necessarie e sufficienti per lo svolgimento del servizio; ad esempio, l'amministratore di un sistema database accede al sistema attraverso la sua utenza personale.

## 2.4. UTILIZZO DELLE PASSWORD E RESPONSABILITÀ

Di seguito sono riassunte le principali regole da adottare nella scelta delle password personali e nella loro gestione.

1. La password è personale di ogni Autorizzato e non cedibile.
2. È fatto divieto di scegliere una password costituita da una sequenza di caratteri che possano rimandare a parole presenti in un dizionario o comunque parole di senso compiuto.
3. È fatto divieto di scegliere una password facilmente associabile ad informazioni relative all'utente, qualiad esempio il nome di familiari, codice fiscale, numeri di telefono, la user-id, ecc.
4. È fatto divieto di utilizzare sequenze digitate alla tastiera (ad esempio: qwerty o 123456).
5. È fatto divieto di riportare la password da qualche parte (ad esempio, su post–it incollato sul proprio monitor).
6. La lunghezza deve essere al minimo di 8 caratteri e deve essere composta da lettere (maiuscole

E minuscole), numeri e caratteri speciali.
7. È fatto divieto di scegliere password deboli (tutte lettere o numeri uguali).
8. La password non deve essere comunicata mediante messaggi e-mail o altre forme di comunicazione elettronica.
9. Nel caso in cui si sospetti che la propria password sia stata compromessa deve essere immediatamente cambiata.
10. Le credenziali di autorizzazione non utilizzate per più di sei mesi devono essere bloccate. Ciò è valido per quei sistemi che consentono una gestione automatica di tale disposizione attraverso l'impostazione di una policy. L'applicazione di tale policy è responsabilità dell'Amministratore di Sistema.
11. Nel caso di cambio di incarico, dimissioni, o qualora necessario, le user-id saranno disabilitate.
12. L'account potrà essere bloccato qualora venga superato il numero di tentativi di accesso consentiti per garantire la protezione da attacchi "brute-force".

Nei casi in cui la tecnologia utilizzata dal Titolare non consenta di implementare i meccanismi di complessità e robustezza della password richiamati in questo documento, è onere dell'Autorizzato applicare direttamente i criteri minimi di complessità e durata definiti dalle regole sopra indicate.

Il Titolare si riserva di implementare sistemi di verifica del corretto utilizzo delle credenziali con modalità conformi al presente Disciplinare, segnalando all'utente eventuali accessi non coerenti col normale utilizzo.

Di seguito i principi di gestione delle utenze utilizzati dal Titolare.

- Le utenze assegnate all'Amministratore di Sistema devono essere distinte dalle utenze comuni e devono essere catalogate in un documento che ne riporti gli estremi e i relativi responsabili.
- Le utenze di dipendenti che cessano il servizio o utenti esterni che non hanno più rapporti con il Titolare devono essere disabilitate nei modi definiti nell'appendice "gestione delle utenze" alla data della conclusione del rapporto. L'avvio tempestivo delle procedure di cessazione è a carico dell'ufficio del personale e tale disposizione trova ragione d'essere sia per aspetti afferenti alla privacy ed alla protezione dei dati, sia per il contenimento delle spese di licenza sui sistemi informatici.

## 2.5. UTILIZZO DELLA POSTA ELETTRONICA

### 2.5.1 PRINCIPI GENERALI

Il presente capitolo disciplina le condizioni di utilizzo del servizio di posta elettronica aziendale fornito dal Titolare ai propri Autorizzati. Il servizio fornito è funzionale all'espletamento delle attività e si articola nella creazione e rilascio di caselle di posta elettronica ed eventuali servizi accessori.

Il Titolare, per l'erogazione del servizio, può utilizzare anche sistemi o infrastrutture di gestori terzi (di seguito indicato come "Provider").

La casella di posta elettronica, ed eventuali servizi accessori erogati dal Provider (come calendario, contatti, spazi di archiviazione on-line e altri), sono assegnati al singolo Autorizzato e pertanto personali. Gli stessi, tuttavia, sono da intendersi strumenti dell'Organizzazione e non privati, di proprietà del Titolare, e possono essere sottoposti a regime di verifica secondo modalità di controllo svolte nel rispetto del presente Disciplinare e delle normative vigenti.

### 2.5.2 UTENTI DEL SERVIZIO DI POSTA ELETTRONICA

La casella di posta elettronica è fornita alle seguenti categorie di Autorizzati (c.d. caselle personali).

- Personale dipendente in servizio attivo, a tempo determinato o indeterminato, per il periodo di durata del rapporto di lavoro: in tal caso il formato dell'indirizzo di posta elettronica è

iniziale_del_nome.cognome@<dominio>.it (dove dominio è l'identificativo univoco assegnato dal Titolare). Per le regole tecniche di composizione del formato, si rimanda all'art. 2.5.9 del presente Disciplinare.

- Collaboratori interni o esterni: anche in tal caso il formato dell'indirizzo di posta elettronica è lo stesso indicato sopra.

La richiesta di attivazione o conservazione della casella di posta elettronica, effettuata dall'ufficio del personale tramite un'apposita procedura di gestione delle utenze.

MODALITÀ DI ACCESSO E VERIFICA

L'accesso alla casella di posta elettronica è di norma concesso in via esclusiva all'Autorizzato, attraverso credenziali personali (user-id e password) univocamente associate alla casella stessa e gestite esclusivamente dall'Autorizzato sotto la propria responsabilità.

La casella di posta elettronica, essendo uno strumento di lavoro e non privato, può essere sottoposta a regime di verifica da parte del Titolare esclusivamente per le seguenti casistiche:

- in caso di attività connesse alla risoluzione di malfunzionamenti o guasti del servizio;
- al fine di garantire la sicurezza informativa dei dati trattati (ad esempio, la gestione di incidenti di sicurezza e tramite azioni preventive sulla diffusione di messaggi contenenti malware);
- in caso di inchiesta da parte dell'autorità giudiziaria o della polizia giudiziaria;
- in caso di sospetta attività illecita;
- in caso di sopravvenuta e urgente necessità lavorativa.

Nei primi quattro casi sopra citati, l'Amministratore di Sistema avanza motivata richiesta al Titolare del trattamento del dato per poter accedere alla casella.

Nel caso di sopravvenuta e urgente necessità lavorativa, dove la sopravvenuta e urgente necessità lavorativa è determinata dall'assenza prolungata dell'Autorizzato e da improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare l'inoltro automatico su altre caselle dell'Organizzazione, la richiesta deve pervenire dal responsabile di area e viene sottoposta al Titolare per il tramite dell'Amministratore di Sistema. Una volta autorizzato l'accesso, questo avviene tramite il meccanismo di delega, che consente al Titolare di delegare l'Amministratore di Sistema, e l'eventuale responsabile di area, all'accesso alla casella con le proprie credenziali ed in modalità tracciata per il tempo necessario alla definizione dell'intervento. Il delegato può leggere, inviare o eliminare messaggi; queste azioni saranno riconducibili al delegato. Il meccanismo di delega garantisce di non divulgare o modificare le credenziali della casella delegata. L'accesso per delega viene notificato all'Autorizzato assegnatario della casella. La casella di posta elettronica mette a disposizione dell'Autorizzato un'apposita funzionalità che consente di inviare automaticamente, in caso di assenza, messaggi di risposta contenenti modalità di contatto alternative.

### 2.5.3 DISPONIBILITÀ DELLA CASELLA DI POSTA ELETTRONICA

La casella personale viene concessa agli assegnatari fintanto che il loro status di Autorizzato al trattamento, così come definito nell'art. 2.5.2, è attivo, salvo i casi di sospensione del servizio previsti dall'art. 2.5.5.

Valgono altresì le seguenti regole in funzione di alcuni stati che caratterizzano il rapporto fra l'Autorizzato e il Titolare.

- Conclusione del rapporto di lavoro o di collaborazione. La casella viene inibita completamente all'invio e alla ricezione della posta a partire dalla data di cessazione della collaborazione/del rapporto di lavoro e mantenuta attiva sino a un massimo di un mese dalla data di conclusione del rapporto di lavoro/del termine della collaborazione. Trascorso tale termine, la casella viene cancellata e così di conseguenza i relativi dati, qualora consentito dai vincoli normativi derivanti dalla natura

pubblica dell'Ente. Dalla data di cessazione della collaborazione/del rapporto di lavoro sino alla data di cancellazione della casella, come sopra individuata, il sistema genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo e-mail aziendale.
Prima della cessazione - a qualsiasi titolo - della collaborazione/del rapporto di lavoro con l'Ente, fermo restando l'obbligo, in capo all'Autorizzato, di rispettare la normativa vigente in materia di archiviazione e conservazione degli atti amministrativi (ivi incluso l'obbligo di protocollare regolarmente tutte le comunicazioni e i documenti rilevanti sulla base delle indicazioni fornite dall'Ente), l'Autorizzato è tenuto a salvare su client locale di posta elettronica eventuali comunicazioni e-mail e/o altro materiale presente nel proprio account di posta elettronica che risultino necessari, anche solo potenzialmente, per le esigenze operative e/o gestionali dell'Ente.

- Distaccamento o aspettativa. La casella viene inibita all'invio della posta verso destinatari esterni al proprio dominio di posta a partire dalla data di inizio del distaccamento/aspettativa. Tale funzionalità verrà ripristinata a partire dalla data di ripresa del servizio presso l'Organizzazione.
- Violazione del Disciplinare: verrà valutata la gravità della violazione del presente Disciplinare per stabilire quali funzionalità della casella di posta elettronica verranno eventualmente revocate.

### 2.5.4 CASELLE IMPERSONALI

Oltre a quanto previsto dall'art. 2.5.2, la casella di posta elettronica viene altresì fornita ad aree, gruppi di lavoro, unità lavorative e strutture organizzative (c.d. caselle impersonali); in tal caso il formato dell'indirizzo di posta elettronica è denominazione@<dominio.it>.

Il Titolare promuove l'utilizzo delle caselle impersonali ai fini di una migliore organizzazione del lavoro.

Le caselle impersonali vengono rilasciate su richiesta del Titolare o del responsabile di area. Il richiedente assume il ruolo di proprietario pro-tempore responsabile della casella di posta e risponde del suo corretto utilizzo ai sensi del presente Disciplinare, in maniera del tutto analoga al caso di una casella personale.

Il proprietario può concedere l'accesso alla casella ad ulteriori collaboratori, esclusivamente attraverso il meccanismo di delega di cui all'art. 2.5.3; i singoli Autorizzati abilitati rispondono dell'utilizzo ai sensi del presente Disciplinare. La casella impersonale rimane attiva fino a richiesta di disattivazione da parte del proprietario fatti salvi i casi di sospensione del servizio previsti dall'art 2.5.5.

### 2.5.5 SOSPENSIONE DEL SERVIZIO

Il Titolare può sospendere temporaneamente l'utilizzo della casella di posta elettronica nei seguenti casi:

- mancata osservanza del presente Disciplinare da parte dell'Autorizzato;
- distaccamento o aspettativa;
- mancato utilizzo della casella da parte dell'Autorizzato per un periodo superiore a sei mesi.

### 2.5.6 AMBITI DI RESPONSABILITÀ DEL TITOLARE

Il Titolare si impegna ad utilizzare i Dati identificativi dell'Autorizzato ai soli fini dell'erogazione e della gestione del servizio. Tali dati saranno protetti nel rispetto della normativa vigente in materia di trattamento dei dati personali. Fatto salvo quanto previsto dall'art. 2.5.5, il Titolare si impegna, con il supporto del Provider, a erogare il servizio in modo continuativo, ad eccezione di sospensioni dovute a:

- ordinaria o straordinaria manutenzione;
- malfunzionamenti ed eventi imprevisti ed imprevedibili;
- interventi per motivi di sicurezza.

Il Titolare attua tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita di informazioni. In ogni caso il Titolare non è responsabile in relazione alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione di messaggi di posta elettronica o di altri contenuti, derivanti da guasti e/o malfunzionamenti degli apparati di gestione e, in generale, dall'erogazione del servizio di posta elettronica stesso o degli eventuali servizi aggiuntivi forniti dal Provider.

Il Titolare non è responsabile in caso di mancata memorizzazione di messaggi, in arrivo o in partenza, per le singole caselle di posta elettronica a seguito di eccesso degli eventuali limiti di spazio messi a disposizione per la casella di posta elettronica.

### 2.5.7 AMBITI DI RESPONSABILITÀ DELL'AUTORIZZATO

La casella di posta elettronica è lo strumento dedicato alle comunicazioni di carattere aziendale e pertanto gli Autorizzati si impegnano ad utilizzarlo per tali finalità. L'Autorizzato si impegna a non utilizzare i servizi oggetto del presente Disciplinare per scopi illegali, non conformi alle indicazioni prescritte o che comunque possano recare danno o pregiudizio al Titolare e/o a terzi.

L'Autorizzato si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio. In particolare, l'Autorizzato non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, immagini, video, audio, codice eseguibile, ecc.), messaggi che esulino dall'esercizio delle proprie mansioni quali, a titolo esemplificativo e non esaustivo, messaggi che contengano o rimandino a:

- pubblicità non istituzionale, manifesta o occulta;
- pubblicità e/o richieste di finanziamenti a favore di altre realtà o strutture esterne;
- comunicazioni commerciali private;
- materiale pornografico o simile, in particolare in violazione della Legge n. 269 del 1998 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù" e ss.mm.ii.;
- materiale discriminatorio o lesivo in relazione a razza, sesso, religione, ecc.;
- materiale che violi la normativa sulla privacy;
- contenuti o materiali che violino i diritti di proprietà di terzi;
- contenuti diffamatori o palesemente offensivi.

L'Autorizzato, inoltre, non può utilizzare il servizio in modo da pregiudicare o interferire con il corretto funzionamento del sistema di posta elettronica e con l'utilizzo del servizio da parte degli altri Autorizzati. In nessun caso l'Autorizzato potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

L'Autorizzato non può tentare di accedere alle caselle di posta elettronica per le quali non è autorizzato, tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti. In caso di rilevazione di minaccia il servizio verrà sospeso.

Il Titolare si riserva la facoltà di segnalare agli organismi competenti, per gli opportuni accertamenti e provvedimenti del caso, le eventuali violazioni alle condizioni di utilizzo della posta elettronica esplicitate nel presente Disciplinare.

### 2.5.8 RISERVATEZZA DELLA POSTA ELETTRONICA

Il Titolare persegue la riservatezza e l'integrità dei messaggi durante il loro transito e la loro permanenza nel sistema di posta.

In particolare, l'Amministratore di Sistema non può accedere ai contenuti delle caselle di posta elettronica salvo autorizzazione scritta del Titolare ed unicamente nel caso in cui ricorrano le condizioni previste dal presente disciplinare. Limitatamente a quanto consentito dal Provider, il Titolare potrà avvalersi di strumenti automatici (anti-spam, anti-virus, ecc.) idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.

### 2.5.9 REGOLE TECNICHE DEL FORMATO DEGLI INDIRIZZI DI POSTA ELETTRONICA

In linea generale si assume quale principio inderogabile che, in caso di omonimie nella definizione degli indirizzi di posta elettronica, la casella che dovrà differenziarsi sarà l'ultima richiesta in ordine temporale, indipendentemente da qualifiche e ruoli del richiedente. In assenza di omonimia, nella definizione del formato standard dell'indirizzo di posta elettronica nome.cognome@<dominio.it>

valgono le seguenti regole:

- cognomi composti vengono concatenati senza separatori (ad esempio, maria rossi bianchi diventa maria.rossibianchi), limitatamente ai primi due cognomi (dal terzo in poi vengono trascurati);
- nomi multipli vengono concatenati senza separatori (ad esempio, maria giovanna rossi diventa mariagiovanna.rossi), limitatamente ai primi due nomi (dal terzo in poi vengono trascurati);
- i caratteri speciali non ammessi dal formato della posta verranno esclusi;
- i caratteri accentati verranno sostituiti dai corrispondenti caratteri non accentati.

### 2.5.10 CONTENUTI SOSPETTI O INSOLITI

Allo scopo di garantire la sicurezza del Sistema Informativo, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare l'Helpdesk per una valutazione dei singoli casi.

### 2.5.11 POSTA ELETTRONICA CERTIFICATA (PEC)

La Posta Elettronica Certificata (PEC) è il sistema di posta nel quale al mittente viene fornita, in formato elettronico, la prova legale dell'invio, della consegna e dell'integrità della e-mail nonché dei documenti informatici (eventuali allegati).

La Posta Elettronica Certificata è un sistema di comunicazione simile alla posta elettronica standard, a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere un valore legale ai messaggi: la comunicazione ha valore legale solo se inviata da una casella PEC e ricevuta da un'altra casella PEC.

La PEC sostituisce, dal punto di vista tecnico e legale, la raccomandata postale con ricevuta di ritorno (il valore legale è sancito dal D.P.R. n. 68 dell'11 febbraio 2005); gli Autorizzati, in base all'organizzazione interna e all'area di appartenenza, hanno pertanto l'obbligo di controllare regolarmente le caselle PEC a loro assegnate, inoltrando al protocollo quanto necessita di essere protocollato.

Il responsabile di area ha invece il compito di organizzare un sistema atto a garantire continuità operativa in particolar modo in caso di assenza prolungata di un Autorizzato.

### 2.5.12 TRASMISSIONE DEI DATI PERSONALI, ANCHE PARTICOLARI

È fatto divieto di trasmettere o ricevere ogni dato personale, anche particolare, proprio o di terzi, attraverso il sistema di posta elettronica messo a disposizione del Titolare; tale prescrizione, che discende direttamente dal GDPR, trova ragione nell'impossibilità di tracciare e discriminare l'accesso al dato soprattutto quando l'interlocuzione avviene con indirizzi e-mail esterni.

Qualora la tecnologia lo consenta, sotto la responsabilità dell'Amministratore di Sistema, il Titolare applica controlli automatici atti a prevenire la possibilità di inviare dati di carattere personale, anche particolare.

In maniera esemplificativa e non esaustiva si evidenzia che:

- codici fiscali (vedasi il parere del Garante sull'uso e la diffusione della Carta nazionale dei servizi – 9 luglio 2003);
- IBAN;
- certificati medici;
- buste paga;

- documenti di identità

non possono essere trasmessi tramite e-mail in chiaro né tantomeno possono essere presenti negli allegati.

In caso di necessità, solo per i dati per cui l'Autorizzato ha ricevuto un preciso incarico al Trattamento da parte del Titolare, sotto la propria responsabilità, può scambiare tali dati attraverso messaggi di posta elettronica crittografati.

Sono esclusi da tale regime i dati inviati e ricevuti tramite PEC, in quanto tale strumento garantisce certezza del soggetto che effettua l'invio e di quello che riceve il dato.

Per la trasmissione di dati personali propri o di congiunti, l'Autorizzato è tenuto ad utilizzare una casella di posta privata e dunque a non utilizzare il sistema di posta elettronica messo a disposizione dal Titolare.

## 2.6. TUTELA DELLA PRIVACY DEI DIPENDENTI

Al fine di tutelare la privacy del personale dipendente (e dei collaboratori in genere, anche esterni), è fatto divieto, nelle aree di rete condivise, di memorizzare file personali – come, ad esempio, copia di documenti di identità, foto e filmati di persone, ecc.

Tale limitazione non è applicata alle aree di memorizzazione messe a disposizione dell'Autorizzato e correlate al profilo personale: ad esempio, hard-disk e desktop sulle postazioni di lavoro in quanto destinate anche all'uso personale e quindi sotto l'esclusiva responsabilità dell'utente (sempre nel rispetto dei principi sopracitati).

L'Amministratore di Sistema, salvo esplicita autorizzazione da parte del Titolare, non è autorizzato, in alcun modo, ad effettuare il backup dei dati personali degli Utenti; il divieto si estende anche ai dispositivi mobili e in caso di sostituzione di dispositivo, fisso o mobile, l'Helpdesk fornirà all'utente, esclusivamente, istruzioni per l'espletamento dell'operazione.

## 2.7. CONSERVAZIONE DEI DATI

Tutti i dati devono essere conservati esclusivamente per il periodo di tempo strettamente necessario al loro Trattamento in relazione ai vincoli normativi derivanti dalla natura pubblica dell'Ente: tale periodo viene puntualmente specificato dal Titolare nel registro dei trattamenti sottoscritto, per presa visione, da ogni Autorizzato.

La stessa interpretazione vale per le banche dati centralizzate o distribuite.

## 2.8. CONDIVISIONE DI FILE

Il Titolare ha stabilito le seguenti modalità per la condivisione di file:

- condivisione di file contenenti documenti di lavoro ai quali possono accedere più utenti contemporaneamente (principalmente file di tipo Word, Excel e PDF in uso a tutti gli Autorizzati di uno o più aree);
- supporto per file personali, ancorché esclusivamente lavorativi, su aree di rete in modo da potervi accedere da più postazioni;
- condivisione di file ed informazioni, ma anche raccolta interna di dati, tra persone di aree diverse (tipicamente questa modalità, talvolta, viene assolta scambiando una grossa mole di file via e-mail col conseguente intasamento delle caselle di posta elettronica).

Il Titolare mette a disposizione tre specifici strumenti, orientati a soddisfare le sopra citate esigenze:

- per la condivisione abitualmente denominata "**cartella di rete**" è stata predisposta

una infrastruttura informatica, gerarchicamente costituita, che prevede cartelle condivise tra aree diverse con permessi di lettura e scrittura discrezionali. Ciascun utente vi accede tramite una unità disco del computer connesso al dominio, ad esempio S: - dove la lettera è identificativo variabile dell'unità, condivisa con altri collaboratori, nella quale potrà salvare e leggere i file. È assolutamente vietato usare tale area per salvare dati personali non attinenti al lavoro d'ufficio.

- **Sharepoint** è invece una piattaforma di collaborazione che consente di gestire e velocizzare i processi di lavoro, grazie alla possibilità di condividere informazioni e documenti con altri Utenti di altre aree o esterni (ad esempio, clienti e fornitori) aprendo lo stesso documento contemporaneamente per visionarlo e/o modificarlo. Vi è inoltre la possibilità di creare report, liste, archivi, calendari sincronizzati e riunire in un'unica posizione tutte le e-mail di un gruppo di lavoro. Ad ogni utente viene assegnato un profilo con le autorizzazioni per accedere a tutte o ad alcune sezioni della piattaforma. La procedura di creazione di un eventuale sotto sito prevede l'approvazione da parte dell'Amministratore di Sistema che verifica se, dalla descrizione inserita, il sito richiesto non costituisca duplicazione di sistemi già in essere.
- **OneDrive** ancora permette di gestire file e documenti della cartella file personali, ancorché esclusivamente lavorativi, sul cloud e di condividerli con gli altri Autorizzati e gli esterni (ad esempio, clienti e fornitori). Consente inoltre di mantenere in locale sul computer una replica sincronizzata dei file personali ma anche dei file memorizzati nelle cartelle Sharepoint aziendali.

Gli Autorizzati sono tenuti a condividere i file contenenti Dati personali solo dopo aver verificato, sotto la propria responsabilità, che i soggetti destinatari siano autorizzati al Trattamento dei dati stessi.

Si richiede inoltre di favorire la condivisione dei file attraverso l'invio del link al file piuttosto che inviare i file come allegati di posta elettronica così da poter esercitare un migliore controllo sull'accesso ai file stessi.

Si specifica che è ammessa la condivisione solo dei dati esplicitamente condivisi e che gli strumenti messi a disposizione del Titolare non possono in alcun modo essere utilizzati per scopi diversi; pertanto, qualunque file che non sia legato all' attività lavorativa non può essere collocato, nemmeno per brevi periodi, sui sistemi del Titolare.

## 2.9. UTILIZZO DELLA NAVIGAZIONE INTERNET

Gli Autorizzati e gli altri Utenti (stagisti, ospiti fruitori del WI-FI, ecc.) che utilizzano un dispositivo connesso alla rete locale del Titolare possono usufruire del servizio di navigazione Internet.

Su tutta la rete interna (e per tutte le sedi) è fatto divieto agli Autorizzati di connettere i dispositivi a loro assegnati direttamente ad Internet (ad esempio, attraverso un collegamento basato sull'hotspot dello smartphone personale): la connessione deve avvenire sempre e solo tramite il sistema proxy, messo a disposizione del Titolare, che ne protegga e ne tracci le attività.

A tal fine tutti i computer, compresi i server, devono essere configurati, sotto la responsabilità dell'Amministratore di Sistema, in maniera automatica ovvero manuale (solo nei casi in cui la tecnologia non premetta automatismi).

Il proxy identifica l'utente e consente l'accesso ad ogni risorsa cui si vorrà accedere a meno che non si richiedano particolari siti vietati come descritto nel seguito del Disciplinare.

Non possono essere utilizzati programmi che si basino su tecnologia peer to peer o che forniscano funzionalità di proxy "anonimizzante". Sono vietati tutti i software che consentono il controllo remoto della postazione degli Autorizzati se non quelli approvati dall'Amministratore di Sistema. L'Amministratore di Sistema ha la responsabilità, per quanto attuabile attraverso le soluzioni tecniche

a disposizione, di inibire il controllo remoto della postazione dell'Autorizzato attraverso soluzioni non approvate dal Titolare.

È vietato accedere a siti o applicazioni Internet che occupano la banda disponibile in maniera continuativa (ad esempio, web-radio o Youtube™ per l'ascolto della musica), così come non si possono visitare siti orientati al gioco o ad altre attività in evidente contrasto con la propria attività lavorativa. Per inibire gli accessi a siti non ammessi l'Amministratore di Sistema, a seguito dell'autorizzazione del Titolare, implementa filtri automatici che inibiscono i contenuti non ammessi.

## 2.10. WI-FI

Negli uffici del Titolare è presente un servizio WI-FI che fornisce connettività sia agli Autorizzati che agli ospiti: le modalità di utilizzo sono precisate in una procedura dedicata.

È vietato creare reti Wi-Fi direttamente connesse alla rete del Titolare e che ne sfruttino la banda.

È vietato connettere i computer e i telefoni di proprietà del Titolare su una rete Wi-Fi diversa da quella aziendale e contemporaneamente sulla rete del Titolare.

## 2.11. UTILIZZO DI SUPPORTI DI MEMORIA ESTERNI

È vietato l'utilizzo di supporti di memoria (hard-disk, chiavette USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti messi a disposizione dell'Organizzazione, salvo che il supporto utilizzato sia stato fornito dal Titolare o suo delegato e formalmente autorizzato per iscritto. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative, ogni salvataggio deve essere effettuato facendo criptando i dati e nei limiti di quanto prescritto dal Titolare nel caso di specie.

## 2.12. UTILIZZO DEI TELEFONI, FAX, FOTOCOPIATRICI E STAMPANTI

L'Autorizzato è consapevole che gli strumenti di stampa, così come anche il telefono, sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto, ne viene concesso l'uso esclusivamente per tale fine. Si evidenzia che:

1. il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza;
2. qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici e per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare, si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita dal Titolare;
3. per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema;
4. è vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del responsabile di Area;
5. per quanto concerne l'uso delle stampanti gli Utenti sono tenuti a stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative, prediligere le stampanti direte condivise per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili) e preferire la stampa in bianco/nero e fronte/retro al fine di ridurre i costi;
6. quando i documenti che contengono dati riservati vengono diretti a stampanti condivise l'Autorizzato deve avere l'accortezza di non lasciare incustoditi i documenti una volta stampati. Al

fine di favorire questa procedura il Titolare prevede l'utilizzo della funzione di "stampa protetta": in tal modo se si imposta un PIN per un documento quando si stampa da computer, il documento viene tenuto nella memoria della stampante e non viene stampato finché non si immette il PIN corretto nel pannello operativo della stampante stessa.

## 2.13. UTILIZZO DI SISTEMI DI MESSAGGISTICA ISTANTANEA.

Fatta salva specifica autorizzazione scritta del Titolare o del suo delegato, è vietato l'utilizzo di sistemi di messaggistica istantanea (quali, a titolo esemplificativo e non esaustivo, WhatsApp, Messenger, Telegram, etc.) al fine di comunicare o diffondere dati personali trattati dall'ODCEC o contenti informazioni comunque riconducibili all'ODCEC, anche se attinenti allo svolgimento della prestazione lavorativa.

Il divieto di cui sopra opera sia qualora tali sistemi siano installati su dispositivi aziendali sia qualora gli stessi siano installati su dispositivi personali.

Il divieto riguarda sia l'utilizzo di messaggi di testo sia qualsiasi altra modalità attivabile per il tramite del sistema di messaggistica istantanea (ad esempio, messaggi vocali, audio, video, immagini). In particolare, è severamente vietato l'invio, tramite i suddetti sistemi, di documenti o altre immagini contenenti dati personali e qualsiasi altra informazione trattati dall'ODCEC.

La violazione delle regole contenute nel presente paragrafo determina l'applicazione di sanzioni disciplinari. Inoltre, nel caso in cui la violazione sia stata posta in essere mediante l'ausilio di dispositivi aziendali, riconducibili l'ODCEC si riserva il diritto di revocare l'assegnazione di tali dispositivi e/o inibire l'accesso a determinate funzionalità degli stessi connesse alla violazione posta in essere.

## 2.14. VIDEOCONFERENZA

Il Titolare mette a disposizione un sistema per la videoconferenza, la registrazione, distribuzione e archiviazione di contenuti audio, video ed immagini. La gestione delle utenze di accesso al servizio rispecchiale norme che regolamentano le utenze interne del Sistema Informativo. Per usufruire del servizio e dei relativi dispositivi è necessario indirizzare una richiesta all'Helpdesk. Se si intende registrare una conferenza audio-video è necessario chiedere il consenso ai partecipanti all'inizio della sessione di registrazione: quando i partecipanti concedono la registrazione è necessario chiedere di nuovo il consenso all'inizio della registrazione così che venga memorizzato contestualmente alla registrazione stessa.

## 2.15. PARTECIPAZIONE AI SOCIAL MEDIA

1. L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dal Titolare attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli Autorizzati.
2. Fermo restando il diritto della persona alla libertà di espressione, il Titolare ritiene comunque opportuno indicare agli Utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine e il patrimonio, anche immateriale, quanto i propri dipendenti e collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.
3. Il presente articolo deve essere osservato dall'Autorizzato sia che utilizzi dispositivi messi a disposizione dal Titolare, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente o collaboratore dell'Organizzazione.
4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza

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

5. L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali, ad esempio, dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del responsabile di Area nonché dei soggetti interessati.
6. Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Organizzazione, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'attività del Titolare.

## 2.16. MISURE CONTRO IL FURTO DEI DISPOSITIVI

Gli Autorizzati per i quali il Titolare ha disposto l'assegnazione di dispositivi mobili, come ad esempio computer e smartphone, hanno la responsabilità di riporre i dispositivi stessi in sicurezza – sottochiave o in locale sicuro – e di non lasciarli incustoditi.

Gli Autorizzati sono inoltre tenuti ad agganciare sempre i computer al cavo di sicurezza per i computer per cui il Titolare abbia previsto il kit antifurto.

È responsabilità degli Autorizzati, previa autorizzazione del Titolare, accedere al locale CED provvedere a collocare e a mantenere sottochiave, in armadi rack, tutti i sistemi server e gli apparati.

È responsabilità dell'Amministratore di Sistema fare in modo che venga applicata la cifratura dei dati memorizzati sui dischi dei dispositivi mobili.

## 2.17. RESTITUZIONE DEI DISPOSITIVI

In caso di cessazione del rapporto di collaborazione/lavoro con il Titolare, l'Autorizzato deve immediatamente restituire tutti i dispositivi, l'attrezzatura, le informazioni e i Dati di cui è entrato in possesso nell'ambito dell'esercizio del proprio incarico.

## 2.18. SALVAGUARDIA DELLE RISORSE DELL'AZIENDA

Il Titolare effettua controlli aggregati a fronte di ogni anomalia e adotta misure anche puntuali al fine di contenere minacce o disservizi che si possano verificare sulla rete. Ad esito di ogni intervento d'urgenza,anche rivolto al singolo utilizzatore, viene redatta dall'Amministratore di Sistema apposita relazione che resta agli atti e viene inoltrata al responsabile di Area per l'utenza coinvolta.

A fronte della rilevazione di comportamenti illeciti, in conformità alla normativa privacy ed al GDPR, il Titolare, con il tramite dell'Amministratore di Sistema, procede a comunicare all'intera organizzazione (o agli Autorizzati interessati) l'invito ad attenersi all'uso previsto per i sistemi informatici del Titolare. In caso di persistente anomalia, nel rispetto dei principi di pertinenza e non eccedenza, il controllo, per il tramite dell'Amministratore di Sistema, viene compiuto su base individuale e il relativo esito potrà fondare l'eventuale avvio di un'azione disciplinare.

L'Amministratore di Sistema, in ragione delle disponibilità di risorse ed al fine di garantire il costante funzionamento dei sistemi, regola la dimensione delle caselle di posta elettronica e delle aree di rete condivise compreso il cloud.

## 2.19. INOSSERVANZA DEL DISCIPLINARE

La responsabilità delle azioni compiute nell'uso del Sistema Informativo è in capo a ciascun Autorizzato.

Ogni azione posta in essere dagli Autorizzati in violazione del presente Disciplinare potrà essere considerata una violazione della sicurezza e, come tale, potrà comportare la revoca dell'accesso alle risorse informatiche e la segnalazione al Titolare (incidente di sicurezza) il quale valuterà l'avvio di un eventuale procedimento disciplinare.

## 2.20. ULTERIORI RESPONSABILITÀ DEGLI AUTORIZZATI

1. Le risorse informatiche del Titolare devono essere utilizzate per l'assolvimento delle finalità tipiche dell'incarico di lavoro.
2. Il Titolare attiva tutte le procedure automatiche per consentire un adeguato e costante utilizzo del mezzo informatico ai fini aziendali. L'uso di Internet per fini personali è consentito limitatamente ai seguenti principi, la violazione dei quali costituisce illecito disciplinare.
    2.1. L'utilizzo degli strumenti informatici per fini personali non deve incidere negativamente sulla prestazione lavorativa dell'Autorizzato.
    2.2. Le attività svolte a titolo personale non devono porre in capo al Titolare alcuna responsabilità penale, civile o amministrativa. È vietata qualsiasi attività che possa produrre danni alle risorse informatiche e di rete del Titolare, che comporti per l'Organizzazione il coinvolgimento in procedimenti penali, civili o amministrativi o che risulti in contrasto con le regole contenute nel presente Disciplinare.
3. La navigazione verso la rete Internet è riconducibile alla responsabilità dell'utente in quanto è consentita solo in modalità autenticata, e come sopra precisato, solo attraverso un server proxy.
4. Tutto il software utilizzato dall'Organizzazione è originale e regolarmente licenziato dai produttori: è fatto divieto agli Utenti di utilizzare software se non quello configurato dall'Helpdesk sul computer. Nel caso l'Autorizzato, nell'ambito della sua attività lavorativa, necessiti di installare un software non previsto, deve inoltrare una specifica richiesta al Titolare; una volta che il Titolare ha autorizzato la richiesta, l'Helpdesk provvede all'installazione e al contestuale aggiornamento dell'asset. L'Amministratore di Sistema è incaricato di verificare periodicamente la configurazione dei computer e di rimuovere qualunque tipo di software diverso da quello previsto e autorizzato dal Titolare.
5. Gli Autorizzati sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi a cui hanno accesso: in caso di assenze anche brevi (pochi minuti) dalla propria postazione di lavoro l'Autorizzato ha l'obbligo di bloccare il computer. In ogni caso l'Autorizzato è responsabile nel caso in cui lasci un elaboratore incustodito e questo venga utilizzato indebitamente da parte di terzi.

## 2.21. INDAGINI INVESTIGATIVE E CONTROLLI SUGLI STRUMENTI

1. Poiché in caso di violazioni del presente Disciplinare, sia l'Organizzazione, sia il singolo Autorizzato sono potenzialmente perseguibili con sanzioni, anche di natura penale, il Titolare verifica, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio Sistema Informativo. L'Organizzazione, infatti, può avvalersi legittimamente, nel rispetto dello statuto dei lavoratori (art. 4, comma 1), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) a condizione che l'impiego di tali sistemi sia giustificato

da esigenze organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale, e che determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, da effettuarsi nel rispetto della normativa privacy. Resta ferma la necessità, prima dell'installazione di tali sistemi, di conclusione di un previo accordo collettivo con RSA/RSU o, in alternativa, di autorizzazione della sede territoriale competente dell'INL.

2. Tali disposizioni (art. 4 comma 1 Stat. lav.), tuttavia, non trovano applicazione relativamente agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa nonché per gli strumenti di registrazione degli accessi e delle presenze (art. 4 comma 2 Stat. lav.).
3. I controlli devono essere effettuati nel rispetto dell'art. 2 del presente Disciplinare e dei seguenti principi:
   3.1. proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite e verrà svolto nella misura meno invasiva possibile;
   3.2. trasparenza: l'adozione del presente Disciplinare ha l'obiettivo di informare gli Autorizzati sui diritti ed i doveri di entrambe le parti relativamente all'utilizzo delle risorse informatiche aziendali e, in particolare, sulle modalità di effettuazione dei controlli da parte del Titolare;
   3.3. pertinenza e non eccedenza: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali degli Autorizzati, così come la possibilità di controlli prolungati, costanti o indiscriminati.
4. Gli strumenti informatici utilizzati dagli Autorizzati possono essere oggetto di controlli da parte dell'Organizzazione, per il tramite dell'Amministratore di Sistema, qualora tale controllo si rendesse necessario per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nonché per la sicurezza e la salvaguardia del Sistema Informativo, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 3 e 4) e possono permettere al Titolare di prendere indirettamente cognizione dell'attività svolta con gli strumenti stessi.
5. Controlli per la tutela del patrimonio, per la sicurezza del lavoro nonché per la sicurezza e la salvaguardia del Sistema Informativo e controlli per ulteriori motivi tecnici e/o manutentivi (ad esempio, aggiornamento o sostituzione o implementazione di programmi, manutenzione hardware, ecc.): qualora per le finalità qui sopra descritte risulti necessario l'accesso agli strumenti e alle risorse informatiche e alle relative informazioni in essi contenute, il Titolare, per il tramite dell'Amministratore di Sistema, si attiene al seguente processo:
   5.1. avviso generico a tutti gli Autorizzati della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del Sistema Informativo e richiamo all'esigenza di attenersi al rispetto del presente Disciplinare;
   5.2. successivamente, se il comportamento anomalo persiste, il Titolare autorizza l'Amministratore di Sistema, potendo così accedere alle informazioni trattate dal Sistema Informativo con possibilità di rilevare archivi trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività può essere effettuata in forma anonima ovvero tramite controllo del numero IP dell'utente e con l'identificazione dell'Autorizzato che non si attiene alle istruzioni impartite.
   5.3. Qualora il rischio di compromissione del Sistema Informativo sia concreto e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali sopra descritti ai punti 1e 2, il Titolare, unitamente all'Amministratore di Sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.
6. Controlli per esigenze produttive e di organizzazione: si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere ad archivi o informazioni lavorative di cui si è

ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, chat, SMS, ecc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni, il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà alla seguente procedura:

6.1. redazione di un atto da parte del responsabile di Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo strumento;
6.2. incarico all'Amministratore di Sistema di accedere alla risorsa con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che, al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;
6.3. redazione di un verbale che riassuma i passaggi precedenti;
6.4. qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo n. 679/16 "General Data Protection Regulation" e dal D.lgs. n. 196/2003 e successive modifiche ed integrazioni.

# 3. REGOLE PER LA GESTIONE DEI SISTEMI

## 3.1. SOGGETTI COINVOLTI

Sono tenuti a rispettare le seguenti prescrizioni tutti gli Autorizzati che fanno parte dell'Helpdesk: il presente capitolo disciplina infatti, sotto la responsabilità dell'Amministratore di Sistema, le modalità con cui vengono erogati i servizi informatici nei confronti degli Autorizzati.

Si precisa tuttavia che, per le parti di loro competenza, anche gli Autorizzati non facenti parte dell'Helpdesk hanno l'onere di recepire e attuare le disposizioni indicate nel presente capitolo.

## 3.2. OBBLIGHI GENERALI

Nella gestione dei sistemi e nella erogazione dei servizi informatici l'Organizzazione agisce in ottemperanza a quanto riportato nel GDPR, relativamente alle modalità di protezione e controllo degli accessi e Trattamento dei Dati personali e in particolare l'individuazione dei soggetti che effettuano il Trattamento dei Dati personali.

Il Titolare si impegna al rispetto delle prescrizioni del GDPR e, in particolare, ad implementare le seguenti misure:

- Effettuare un DPIA (Data Protection Impact Assessment) che consiste nella valutazione degli impatti sulla protezione dei Dati personali. Questa analisi contiene una descrizione sistematica dei trattamenti previsti e delle finalità del Trattamento, una valutazione dei rischi per i diritti e le libertà degli Interessati e le relative misure di sicurezza previste per contrastare i rischi individuati.
- Mantenere il registro delle attività di Trattamento di Dati personali. Tale registro, tenuto a cura del Titolare, viene messo a disposizione dell'Autorità Garante qualora lo richieda, e contiene:
    - il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del Titolare del Trattamento e del

responsabile della protezione dei dati;
    - le finalità del trattamento;
    - una descrizione delle categorie di Interessati e delle categorie di Dati personali;
    - le categorie di destinatari a cui i Dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;
    - i termini ultimi previsti per la cancellazione delle diverse categorie di Dati;
    - una descrizione generale delle misure di sicurezza tecniche e organizzative.
- Introdurre nei sistemi di progettazione il principio di privacy by design, che consiste nell'implementare misure di carattere sia tecnico che organizzativo per tutelare i diritti dell'Interessato già dalle prime fasi di progettazione ed il principio di privacy by default che implica un approccio alla protezione dei dati personali proattivo e non più reattivo (partire da configurazioni "chiuse" dei sistemi informatici, per poi gradualmente ampliarle solo dopo avere valutato l'impatto di eventuali aperture ovvero le impostazioni predefinite devono essere quelle che garantiscono il maggior rispetto della privacy, affinché i dati personali non siano resi accessibili ad un numero indefinito di persone senza l'intervento umano).

## 3.3. MISURE DI SICUREZZA DEI COMPUTER DEGLI AUTORIZZATI

L'Autorizzato è dotato di un computer (fisso o portatile) con almeno i seguenti dispositivi di sicurezza.

- Agente antivirus collegato alla consolle centrale per la distribuzione degli aggiornamenti.
- Agente software distribution per il patching degli applicativi e per l'installazione di nuovi software.
- Agente per la connessione remota, tramite VPN, con la rete del Titolare.

È responsabilità diretta dell'Autorizzato provvedere all'aggiornamento dell'antivirus e al patching del sistema se assegnatario di computer portatile che non venga collegato alla rete del Titolare, direttamente o tramite VPN, per lungo tempo.

Il personale esterno all'Organizzazione può si collegarsi alla rete del Titolare ma solo attraverso i protocolli di sicurezza individuati dall'Amministratore di Sistema: in tal caso, detto personale, e/o la loro organizzazione, deve garantire che le postazioni di lavoro, che utilizzano per accedere alla rete del Titolare, siano protette in maniera analoga alle postazioni dell'Organizzazione garantendone la protezione da virus e malware e l'aggiornamento in termini di patching. L'onere di verifica è dell'Amministratore di Sistema che abiliterà l'utente esterno solo dopo aver verificato e documentato la rispondenza ai criteri sopradescritti.

## 3.4. ASSISTENZA AGLI AUTORIZZATI E MANUTENZIONI

- L'Amministratore di Sistema, e l'Helpdesk sotto la sua supervisione, può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi.
    - Verifica e risoluzione di problemi sistemistici ed applicativi su richiesta dell'Autorizzato.
    - Verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
    - Richieste di aggiornamento software e manutenzione preventiva hardware e software.
- Quando l'intervento richiede l'accesso ad aree personali dell'Autorizzato, gli interventi tecnici devono avvenire previo consenso dell'Autorizzato. Qualora l'intervento tecnico (sia in loco che in remoto) non necessiti di accedere mediante credenziali dell'Autorizzato, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.
- L'accesso in teleassistenza sui computer e sui server della rete, richiesto da terzi (fornitori e/o altri), deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento che rilascerà una autorizzazione specifica limitata al periodo di intervento.
- Durante gli interventi in teleassistenza da parte di operatori terzi, l'Autorizzato ha l'obbligo di

presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente Disciplinare.

## 3.5. REGOLE PER GLI ACCOUNT AMMINISTRATIVI

- Gli account degli Autorizzati devono avere esclusivamente privilegi da utente. La creazione di utenti con privilegi amministrativi deve essere valutata dall'Amministratore di Sistema e comunque sempre autorizzata dal Titolare.
- Deve essere limitato al massimo l'accesso remoto ai server.
- Gli account applicativi devono avere privilegi limitati al solo funzionamento dell'applicazione specifica.
- Ogni applicazione deve avere un proprio account amministrativo.
- L'assegnazione di queste utenze amministrative al personale esterno ha carattere eccezionale e deve essere giustificata ed autorizzata dal Titolare sulla base di contratti di fornitura che richiedano specificatamente tale compito. L'utenza deve essere immediatamente cessata al termine degli incarichi contrattualmente previsti.
- Le password devono essere memorizzate esclusivamente attraverso un sistema che metta a disposizione un database cifrato il cui file deve essere posto sotto backup esclusivo multiplo.

## 3.6. IDENTITY MANAGEMENT

Ogni componente del sistema (ad esempio, OS, DB, applicativo ecc.) deve essere integrato con il sistema di provisioning delle utenze ovvero deve essere connesso a un sistema centralizzato (ad esempio, LDAP). Il sistema di gestione delle credenziali è unico e centralizzato per le credenziali degli Autorizzati.

## 3.7. UTENZE AMMINISTRATIVE NON NOMINALI

Le utenze amministrative non nominali (administrator, root, sys, system, ecc.) vengono sempre disabilitate oppure, in alternativa, le relative password vengono conservate in busta chiusa riposta in luogo sicuro (ad esempio, cassaforte). Gli accessi amministrativi attraverso le utenze amministrative non nominali devono essere sempre preventivamente approvati dal Titolare o suo delegato.

## 3.8. ACCOUNT E PASSWORD POLICY

Il sistema effettua la verifica delle credenziali di autenticazione prima di consentire l'accesso. Il sistema deve implementare regole sulle password e account.

- Password
    - Cifratura delle password memorizzate.
    - Lunghezza minima pari ad almeno 8 caratteri.
    - Almeno tre dei seguenti criteri: un carattere minuscolo, un carattere maiuscolo, un carattere numerico, un simbolo.
    - Divieto di utilizzare le precedenti 5 password.
    - Blocco account dopo 5 tentativi errati.
    - Scadenza dopo al massimo 30 giorni.
    - Cambio password obbligatorio al primo accesso.
- Account
    - Blocco account personali dopo 90 giorni di non utilizzo.
    - Gestione data scadenza account.
    - Ogni utente deve essere univocamente identificato sui sistemi tramite sistema di

gestione delle credenziali.
- La gestione delle utenze interne avviene in maniera centralizzata.

## 3.9. FLUSSI DI COMUNICAZIONE VERSO L'ESTERNO

Tutti gli accessi e/o i flussi di comunicazione, e trasferimento dati, da e verso l'esterno (ad es. verso altre sedi, partners, clienti o fornitori, organizzazioni in genere estranee al Titolare) devono utilizzare canali di comunicazione sicuri e/o cifrati (ad esempio, SFTP, FTPS, https, VPN, ecc.).

Tutti i portali di servizi pubblicati verso l'esterno devono utilizzare protocolli di comunicazione cifrata (ad es. https/TLS, ecc.).

## 3.10. DATI IN AMBIENTE DI SVILUPPO E TEST

I dati presenti sui sistemi dell'ambiente di produzione devono essere logicamente ovvero fisicamente separati dai dati utilizzati per lo sviluppo ed il test anche qualora sia necessario effettuare test in produzione per fini di trouble-shooting.

In tutti gli ambienti di sviluppo e test, i Dati personali degli Utenti non dovrebbero essere utilizzati se non mascherati/anonimizzati opportunamente: ciò è praticabile salvo accertate limitazioni di taluni software o sistemi (ad esempio, ove siano obsoleti e non aggiornati alle ultime disposizioni). In ogni caso, i responsabili di Area hanno l'onere di definire opportune procedure atte a garantire un sicuro Trattamento dei dati in ambiente di sviluppo e test.

## 3.11. AUDIT LOG

Le componenti del sistema (OS, DB, applicativo, ecc.) devono essere integrate, per l'invio dei log, con lo strumento di log collecting. Tutti i log degli amministratori di sistema devono essere automaticamente memorizzati sul sistema di Log Management implementato dal Titolare in ottemperanza al Provvedimento del Garante del 28/11/2008 – (Provvedimento Amministratori di Sistema). In relazione alle capacità di archiviazione dell'infrastruttura l'Organizzazione conserverà i file di log della posta elettronica e della navigazione in Internet per un periodo non superiore a 12 mesi.

I file di log generati devono contenere almeno le seguenti informazioni.

- Utenza che ha generato l'evento.
- Sistema informatico che ha generato l'evento.
- Data ed ora dell'evento (timestamp).
- Tipologia ed esito dell'evento (ad esempio, login, logout, ecc.).

## 3.12. ANTIVIRUS/ANTIMALWARE PROTECTION

Su tutti i dispositivi, compresi evidentemente i server, deve essere attivato un sistema di protezione Antivirus/Antimalware connesso alla consolle centrale per il controllo e gli aggiornamenti. Non è ammesso l'utilizzo di strumenti di protezione se non quello adottato dal Titolare.

## 3.13. DATA ENCRYPTION

I sistemi che conservano dati "critici" (ad es. dati sensibili, PIN, ecc.) devono implementare controlli di cifratura dei dati (a livello OS/DB/applicativo) per garantire la riservatezza delle informazioni. Deve essere prevista una gestione sicura delle chiavi crittografiche (tale per cui la chiave sia conosciuta da un solo soggetto - che ne abbia ricevuto l'incarico - e conservata in modo sicuro).

## 3.14. DATA INTEGRITY

I sistemi che conservano dati "critici" (ad esempio, audit log, ecc.) devono implementare controlli di integrità/firma (ad es. attraverso l'utilizzo di hashing, trusted timestamp, sistemi di controllo/monitoraggio dell'integrità dei file, ecc.).

## 3.15. STRONG AUTHENTICATION

L'accesso a dati critici (ad es. Dati particolari, Dati giudiziari) deve essere protetto da sistemi di strong authentication (basata su due fattori).

## 3.16. RETE E DIFESA PERIMETRALE

L'architettura di rete del Sistema Informativo del Titolare è stata progettata secondo il principio di perimetrazione dei servizi e il controllo degli accessi degli utenti esterni ed interni ai servizi stessi è implementato proprio sull'apparato di sicurezza che delimita i vari perimetri. I componenti per la sicurezza perimetrale, costituiti da Firewall, IPS, IDS, Web Application Firewall e VPN IPSeC, sono distribuiti secondo una logica legata alla topologia dell'infrastruttura di rete. I vari livelli di sicurezza sono:

- Front-end security: apparato a protezione della rete maggiormente esposta all'esterno (Internet) per la gestione controllata degli accessi e l'analisi statefull dei flussi in entrata ed in uscita, oltre l'applicazione di regole specifiche per la pubblicazione dei servizi verso l'esterno.
- Back-end security: apparati e sistemi per la segmentazione e la protezione della rete LAN interna.
- Site to site Security: disciplina per l'interconnessione in sicurezza delle eventuali sedi periferiche dislocate sul territorio, attraverso l'utilizzo di protocolli di comunicazione sicuri per la cifratura dei flussi che attraversano le reti in fornitura di provider esterni.
- Mobile security: disciplina per l'interconnessione in sicurezza delle postazioni mobili con connettività LTE o 3G-4G-5G, utilizzate per applicazioni operative o eventi specifiche su tutto il territorio.
- Wireless security: apparato a protezione di reti senza fili direttamente connesse all'esterno che utilizzano un sistema di autenticazione e associazione sicura dei dispositivi mobili.

L'infrastruttura prevede il suo centro nevralgico presso la sede centrale da cui sono controllati i servizi ICT e che dispone di connettività verso la rete pubblica Internet. Nel caso di sedi secondarie (in forma stabile o temporanea) viene adottata la soluzione di estendere la LAN interna (via VPN site-to-site) e così tutti i protocolli di protezione previsti.

I principi generali delle politiche di sicurezza delle reti, i processi di approvazione nonché le specifiche regole di firewalling sono documentate e mantenute a cura dell'Amministratore di Sistema.

La politica generale del Titolare è di escludere il ricorso ad eccezioni puntuali riconducendo, quindi, ogni necessità ad una delle possibilità tecnicamente supportabili tra le configurazioni disponibili già implementate.

## 3.17. BACKUP DEI DATI

Il Titolare individua due tipologie di backup in ragione dello scopo.

- Backup ai fini di un rapido ripristino del servizio e della continuità operativa (implementato con tecnologie di snapshot e/o di clone ovvero con procedure di riconfigurazione di un nuovo sistema funzionante).
- Backup ai fini di conservare l'evoluzione temporale del dato (implementato con tecnologie di

backup incrementale/full).

Per ciascun sistema in esercizio deve essere implementata, sin dalla messa in produzione, una delle due strategie in ragione del tipo di servizio erogato. In particolare, solo i servizi transazionali necessitano di conservazione mentre i servizi erogati per legge o per funzionalità generale devono adottare la modalità di continuità operativa. Nel piano di continuità operativa vengono definiti, sotto la responsabilità dell'Amministratore di Sistema, i criteri specifici per la scelta della strategia di backup e della tecnologia da utilizzare.

## 3.18. RIPRISTINO DEI DATI

Il Titolare garantisce la conservazione dei dati solo al fine di garantire il ripristino dei servizi e delle informazioni trattate in caso di incidente informatico o di incidente di sicurezza. Le attività di backup e ripristino, essendo molto onerose in termini di risorse di elaborazione, non vengono invece applicate ai dati che gli Utenti possono conservare sui propri computer (ad esempio, sul desktop) o sulle aree personali a loro assegnate; gli Utenti sono i soli responsabili del mantenimento di una copia di questi Dati personali. Il Titolare garantisce la possibilità di recuperare solamente file su cartelle condivise, dati mantenuti sui server ed e- mail erroneamente cancellate o perse per una finestra temporale in misura variabile stabilita dall'Amministratore di Sistema in base ai termini previsti dal GDPR.

## 3.19. ESECUZIONE DI TEST DI RIPRISTINO DEL BACKUP

L'Amministratore di Sistema, sotto il controllo e la responsabilità del Titolare, esegue verifiche del ripristino dei backup con cadenza almeno trimestrale: al termine del test l'Amministratore di Sistema invia al Titolare l'esito dell'operazione.

## 3.20. MONITORAGGIO E CONTROLLI

Il Titolare dispone di una piattaforma di monitoraggio che, attraverso una rete di sensori installati sugli apparati da monitorare, consente di raccogliere le informazioni sulle prestazioni e gli eventuali malfunzionamenti. Gli alert sono notificati all'Helpdesk per la relativa escalation.

## 3.21. DISASTER RECOVERY

I dati, le informazioni e le applicazioni che li trattano sono parte essenziale ed indispensabile per l'Organizzazione e pertanto diventano un bene primario da salvaguardare attraverso l'adozione di misure che garantiscano la disponibilità dei dati, indipendentemente dagli eventi che possono presentarsi.

Il coordinatore del Disaster Recovery/Business Continuity è l'Amministratore di Sistema. È una posizione permanente che collabora con tutti i responsabili di Area per la redazione e la revisione periodica di aggiornamento delle rispettive parti del piano.

L'Amministratore di Sistema è, inoltre, responsabile di:

- provvedere, coadiuvato dai responsabili delle varie aree, all'individuazione e alla nomina delle persone chiave di ogni funzione e ad integrare ed aggiornare l'elenco di raccordo fra funzioni e nominativi;
- pianificare specifici incontri con l'obiettivo di informare il personale individuato sui rispettivi compiti;
- verificare le risorse a disposizione e valutarne le caratteristiche per determinarne l'adeguatezza a soddisfare le esigenze di ripristino della operatività dell'Organizzazione.

La revisione del piano deve essere inoltre attuata ogni volta che ognuna delle componenti hardware, software (applicativo e di sistema), di rete e organizzative subiscono un aggiornamento significativo.

A tale scopo tutti i responsabili di Area coinvolti nel piano devono provvedere alla manutenzione della propria componente del piano ovvero inoltrare all'Amministratore di Sistema la comunicazione scritta delle modifiche avvenute per aggiornare il piano stesso.

L'Amministratore di Sistema, una volta verificata e consolidata la modifica del piano, provvede a trasmettere il piano aggiornato al Titolare.

## 3.22. AGGIORNAMENTO DEI SISTEMI

- Client: la gestione della sicurezza logica delle postazioni di lavoro è implementata attraverso uno strumento centralizzato e trasparente per l'utente. Tutte le postazioni di lavoro sono assoggettate a un dominio. Ogni postazione di lavoro collegata all'Active Directory, tramite le policy di dominio, riceve gli aggiornamenti.
- Server: la gestione degli aggiornamenti dei server, vista l'importanza dei servizi erogati, non può essere demandata a delle procedure automatiche. In questo caso è previsto un processo che preveda la produzione di un piano temporale da parte dell'Amministratore di Sistema (basato essenzialmente sulla criticità dei servizi erogati dai server) e, nell'eventualità, la raccolta di evidenze che giustifichino l'impossibilità di implementare alcuni aggiornamenti sui server. Ogni variazione del piano deve essere approvata dal Titolare.

## 3.23. CONFIGURAZIONE STANDARD SICURA

I computer dell'Organizzazione vengono gestiti secondo le policy qui riepilogate in sintesi:

- Configurazione computer.
  - Tutti i dispositivi sono identificati in maniera univoca sulla rete del Titolare utilizzando lo schema OCCLTXX (dove OC è la sigla univoca che identifica il Titolare e XX è un progressivo che individua unicamente il dispositivo). I Server utilizzano invece lo schema OCSRVXX. Non è consentito utilizzare un sistema di identificazione diverso da quello previsto.
  - Non è consentito all'Autorizzato di modificare le caratteristiche impostate sulle postazioni di lavoro assegnate.
- Configurazione stampanti.
  - Le stampanti devono essere collegate con cavo USB al computer o, se predisposte con interfaccia, alla rete del Titolare. Il software dei driver deve corrispondere a marca e modello della stampante.
  - Se non si dispone di una stampante locale devono essere utilizzate le stampanti di rete dislocate nell'Area di appartenenza.
- Dominio e rete.
  - Per accedere alla rete e ai suoi servizi, tutti i computer, senza esclusione alcuna, devono appartenere al dominio del Titolare. I computer di soggetti esterni che si connettono alla rete WI-FI lo fanno attraverso una rete riservata e isolata dalla rete del Titolare.
  - Eventuali connessioni al dominio di computer non di proprietà del Titolare saranno autorizzate dall'Amministratore di Sistema previa verifica e adeguamento eventuale dei software che gestiscono gli ambiti di sicurezza.
  - Computer disgiunti dal dominio o configurati come collegati ad altri domini saranno abilitati ad un numero ristretto di servizi.
  - Tutti i computer connessi con la rete del Titolare assumono la configurazione dinamica dell'indirizzo IP tramite server DHCP. È vietata la configurazione di un indirizzo IP statico della scheda di rete. Nel caso in cui si ha la necessità di riservare un determinato indirizzo IP va effettuata richiesta all'Helpdesk che, con la supervisione dell'Amministratore di Sistema, ne

valuterà la fattibilità tecnica e la reale necessità; ogni qualvolta sia possibile gestire l'esigenza con indirizzamento dinamico sarà negata l'autorizzazione.

- Server.

I sistemi server sono sottoposti ad un processo di "hardening" mediante le seguenti direttive.

- Eliminazione dei servizi non espressamente richiesti dall'ambito a cui è dedicato il server.
- Rimozione di tutte le componenti (pacchetti applicativi, esempi, documentazione, utenze predefinite, ecc.) non indispensabili all'erogazione del servizio.
- Disattivazione di tutte le politiche di routing tra le interfacce di rete (no IP forwarding).
- Costante e tempestivo aggiornamento del sistema operativo e delle applicazioni alle ultime versioni rese disponibili dai produttori, in modo da minimizzare il rischio legato alle nuove vulnerabilità.
- Attivazione dell'auditing e logging di tutti i tipi di accessi su server centralizzato.
- Policy delle password a scadenza programmata.
- Password su bios e firmware che impedisce al personale che ha avuto accesso alla sala CED, ad esempio per interventi di manutenzione, di inserire dischi di avvio non autorizzati.
- Restrizione degli accessi a tutti i file di sistema e/o critici e disabilitazione dell'accesso via rete di utenti privilegiati.
- Attivazione di un meccanismo di sincronizzazione dell'ora dei sistemi per assicurare meccanismi di log e audit coerenti e significativi.

## 3.24. INVENTARIO DEI DISPOSITIVI E AGGIORNAMENTISOFTWARE

La gestione degli asset avviene mediante l'utilizzo di strumenti che permettono l'inventario dei dispositivi ma anche l'attività di update and patch management.

Le postazioni di lavoro, i server, gli apparati di rete e in generale tutti gli asset sono inventariati e presenti all'interno dell'archivio centrale mantenuto sempre aggiornato sotto responsabilità dell'Amministratore di Sistema e su cui si fanno periodiche verifiche.

## 3.25. RIASSEGNAZIONE DEI DISPOSITIVI

Ogni qualvolta un dispositivo informatico viene ridestinato ad un nuovo Autorizzato l'Amministratore di Sistema deve mettere in atto un intervento tecnico preventivo volto a garantire che gli eventuali dati precedentemente memorizzati vengano eliminati e risultino così tecnicamente irrecuperabili.

È responsabilità dell'Amministratore di Sistema fare in modo che tale pratica venga applicata sui dispositivi che vengono dismessi.

## 3.26. NAVIGAZIONE INTERNET

L'accesso ad Internet dalla sede del Titolare avviene in modalità autenticata. L'Autorizzato, mediante un meccanismo di sigle-sign-on, una volta che, tramite il proprio account, accede ai servizi informatici, per la navigazione web dalla sede deve utilizzare sempre e solo il sistema di proxy (non è consentito l'accesso diretto ad Internet) messo a disposizione dal Titolare. I file di log relativi alla navigazione riporteranno la data e l'ora di accesso dell'utenza e l'indirizzo della risorsa acceduta, eventuali tipi di file caricati o scaricati e la dimensione; non viene memorizzata alcuna informazione relativa ai contenuti fruiti dall'utente. Per proteggere il Sistema Informativo da minacce informatiche è presente un ulteriore sistema di controllo tramite un sistema di web-filtering per:

- bloccare le minacce presenti sulla rete Internet nell'ottica di ridurre le infezioni da malware e diminuire il rischio di incidenti;
- bloccare l'accesso a siti ludici quali quelli categorizzati come porno, giochi on line, streaming video

di contenuto ludico;
- bloccare l'uso di applicazioni di controllo remoto;
- limitare l'uso della banda su sistemi esterni quali streaming video e audio, anche se istituzionali, e social network al fine di garantire un livello minimo assicurato di servizio per la fruizione di siti necessari all'Autorizzato nell'ambito dello svolgimento del proprio lavoro.

## 3.27. ACCESSO IN VPN

Agli Autorizzati è consentito svolgere la prestazione in modalità smart working solo se autorizzato dal Titolare e connettendosi solo tramite strumenti standard forniti dallo stesso. l'Autorizzato accede alla rete utilizzando la tecnologia VPN in modalità client to site. È possibile consentire l'accesso da remoto alla rete del Titolare anche a soggetti esterni (partners, stagisti, tirocinanti, terze parti, ecc.). In questo caso la richiesta deve essere autorizzata dal Titolare previo: analisi di fattibilità tecnica da parte dell'Amministratore di Sistema, coerenza con il presente Disciplinare circa le modalità di accesso, identificazione puntuale dei soggetti ed il necessario isolamento rispetto al contesto dei sistemi informativi del Titolare. L'Autorizzato il quale svolga la prestazione in modalità smart working presta la propria opera con diligenza e riservatezza attenendosi alle istruzioni ricevute dal responsabile dell'Area con cui collabora, relativamente ai mezzi e agli strumenti di lavoro utilizzati, ed in particolare ha cura di un utilizzo riservato di eventuali codici di accesso ai server e ai relativi strumenti di lavoro.

Dalla rete del Titolare non è possibile connettersi a VPN esterne se non in casi autorizzati e censiti dall'Amministratore di Sistema a seguito dell'analisi di fattibilità tecnica e di coerenza con il presente

Disciplinare circa le modalità di accesso, l'identificazione puntuale dei soggetti ed il necessario isolamento rispetto al contesto dei sistemi informativi del Titolare.

## 3.28. ACCESSO AL LOCALE CED

I sistemi server sono collocati in un apposito locale (CED) che garantisce la continuità di servizio grazie anche ad un impianto di condizionamento ambientale e una linea elettrica dedicata supportata dal gruppo di continuità.

L'accesso al locale CED è consentito solo agli Autorizzati che hanno ricevuto una specifica autorizzazione da parte del Titolare: è responsabilità di tali Autorizzati che il locale venga mantenuto sempre chiuso a chiave durante la loro assenza.

Il Titolare dispone in merito alla conservazione di una copia della chiave di accesso, in luogo sicuro e utile nel caso in cui si renda necessario accedere al locale per una emergenza. Il Titolare cura altresì il censimento delle chiavi di accesso e della relativa assegnazione.