ASP CITTÀ DI BOLOGNA
Azienda pubblica di servizi alla persona

REGOLAMENTO PER L'UTILIZZO DELLE RISORSE INFORMATICHE DI ASP CITTÀ DI BOLOGNA - Azienda pubblica di Servizi alla Persona

Adottato con Atto di Delibera dell'Amministratore Unico n. 17/2024 (All. A)

ASP Città di Bologna
Sede legale
Via Marsala, 7 - 40126 Bologna
Sede amministrativa
Viale Roma, 21 - 40139 Bologna - Tel. +39.051.620.13.11
Sito WEB: www.aspbologna.it

Indice

1. Normativa di riferimento 5
1.1. Principali riferimenti normativi 5
1.2. Principali riferimenti Aziendali 5
2. Premessa 6
3. Le principali definizioni 7
4. Oggetto e campo di applicazione 10
5. I principi 10
6. I divieti 11
7. Responsabilità 12
7.1. Procedure informatizzate autorizzate 12
7.2. *Data breach* 12
7.3. Procedure informatizzate non gestite dal S.I. 13
8. Sistemi di autenticazione e di autorizzazione 13
8.1. Credenziali di autenticazione (coppia username e *password*) 13
8.2. Accesso agli applicativi Aziendali 13
8.3. Gestione delle credenziali 13
8.4. Sistema d'autorizzazione per le procedure informatizzate distribuite dal S.I. 15
8.5. Designazione Trattamento Dati Personali 16
9. Norme generali per l'utilizzo delle Risorse Informatiche 16
9.1. *Computer* aziendali 16
9.2. *Computer* portatili aziendali 17
9.3. Utilizzo di attrezzature informatiche personali 17
9.4. Stampanti, *scanner* e fotocopiatrici multifunzione 18
9.5. Supporti di memorizzazione: CD, DVD, *hard disk* esterni, *memory card*, *pen drive* 19
9.6. Norme generali per l'utilizzo del *software* distribuito dal S.I. 20
9.7. *Softwar*e *antivirus* e di protezione dei Dati 20
9.8. Dischi di rete, cartelle personali e cartelle condivise 21
10. Collegamento di attrezzature alla rete Dati 22
10.1 Rete di ASP 22
10.2. Altre reti *Wi-Fi* in ASP 22
11. Uso e salvataggio dei Dati Aziendali (*backup*) 22
11.1. Supporti di memorizzazione: CD, DVD, *hard disk* esterni, *memory card*, *pen drive*.) 23
12. Utilizzo della posta elettronica 23
12.1. Definizioni e strumenti 23
12.2. Attribuzione della casella personale di posta elettronica aziendale 25

12.3. Utilizzo della posta elettronica aziendale 25
12.4. Attribuzione della casella PEC 26
12.5. La tutela della riservatezza 26
12.6. Invio tramite *e-mail* di documentazione sanitaria 26
12.7. Le regole di buon comportamento per l'utilizzo delle caselle *e-mail*. 26
12.8. Considerazioni sull'attendibilità dell'identità del mittente di posta elettronica 28
12.9. Sistemi di sicurezza 28
12.10. Gestione della casella di posta elettronica in caso di assenza dell'Utilizzatore/Utente 29
12.11 28
12.12. Accesso alla casella di posta elettronica per ragioni di sicurezza o manutenzione 30
13. Utilizzo della rete *Internet* 30
13.1. Definizioni e strumenti 30
13.2. Abilitazione alla connessione *Internet* 31
13.3. Utilizzo delle connessioni a *Internet* 31
13.4. Regole di buon comportamento per l'utilizzo di *Internet* 32
13.5. Responsabilità in merito all'utilizzo di *Internet* 33
13.6. Responsabilità in merito all'accesso a *Internet* 33
13.7. Revoca delle credenziali o dei diritti di accesso a *Internet* 33
13.8. Sistemi di sicurezza e categorie di siti bloccate da sistemi automatici 34
13.9. Pubblicazione di contenuti e realizzazione di siti personali 34
13.10. Connessione a *provider* diversi da quello aziendale 35
13.11. Utilizzo di *server* esterni per *backup*, gestione, e condivisione dei documenti aziendali 35
13.12. Assistenza da remoto (VPN e altre tipologie) 35
13.13. Utilizzo delle cartelle condivise 35
14. Utilizzo dello *smartphone* aziendale 36
15. Modalità di prestazione dei servizi 36
16. Installazione di *Microsoft Office* sulle postazioni di lavoro 37
17. Utilizzo dei sistemi di videoconferenza 37
18. Lavoro Agile (c.d. *Smartworking*) 37
19. Gli strumenti di controllo 37
19.1. L'utilizzo dei sistemi *software* applicativi aziendali. 37
19.2. Gli accessi a *Internet* 38
19.3. L'utilizzo della posta elettronica 38
19.4. La telefonia 38
19.5. La registrazione delle conversazioni telefoniche 39
19.6. Facoltà di ASP 39
19.7. Limite dei controlli 40
19.8. Cessazione della disponibilità dei servizi informatici aziendali 40

19.9. Responsabilità dell'Utilizzatore delle risorse informatiche 40
19.10. Finalità e modalità del Trattamento 41
19.11 Comunicazione e diffusione 41
20. *Focus*: utilizzo dei mezzi di informazione e dei *social media* 41
21. L'accessibilità 42
21.1. Premessa 42
21.2. L'accessibilità in ASP Città di Bologna 42
22. Responsabilità disciplinare 42
23. Osservanza delle disposizioni in materia di *Privacy* (GDPR) 43
24. Aggiornamento e Revisione 44
25. Rinvio 44
Allegato 1 Elenco applicativi di base e specifici autorizzati in uso in ASP Città di bologna 45

1. Normativa di riferimento

1.1. Principali riferimenti normativi

- *Regolamento Generale per protezione dei Dati*" (UE) 679/2016 ed ev. ss. mod. e int. ("GDPR")
- D. Lgs. 196/2003 come modificato dal D.Lgs.101/2018 "*Codice in materia di protezione dei Dati personali*" ed ev. ss. mod. e int.
- Decreto Legislativo 7 marzo 2005 n. 82 "*Codice dell'amministrazione digitale*" e s.m.i.
- D.P.R .13 Giugno 2023, n.° 81 "*Regolamento concernente modifiche al D.P.R. 16 aprile 2013, n. 62, recante Codice di Comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*".
- D.P.R. 11 febbraio 2005, n° 68 *"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*" ed ev. ss. mod. e int.
- Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri-Dipartimento della funzione pubblica: "*Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro*".
- Direttiva del 18 novembre 2005 "*Linee Guida per la Pubblica amministrazione digitale*".
- Direttiva 27 novembre 2003 del Dipartimento per le innovazioni e la tecnologia "*Impiego della posta elettronica nelle pubbliche amministrazioni*".
- Circolari AgID n° 1 e 2/2017[1].
- Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 "*Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei Dati personali*".
- Deliberazione 13 del 1 Marzo 2007 "*Lavoro: le linee guida del Garante per posta elettronica e internet*".
- Piano triennale AgID[2].
- Legge n° 300 del 20/05/1970 e s.m.i c.d. "*Statuto dei lavoratori*".
- Legge 23 dicembre 1993 n. 547- "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*".

1.2. Principali riferimenti Aziendali

- PIAO (PIANO INTEGRATO DI ATTIVITÀ ED ORGANIZZAZIONE AZIENDALE)[3]

[1] http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg
[2] https://pianotriennale-ict.italia.it/
[3] reperibile su Amministrazione Trasparente al seguente link: Atti generali - ASP Città di Bologna (aspbologna.it)

2. Premessa

ASP Città di Bologna - Azienda pubblica di Servizi alla Persona, con sede legale a Bologna - 40126, via Marsala, n. 7 e sede amministrativa in Bologna -040139, via Roma, n. 21, P. IVA e C.F.: 03337111201, *e-mail* di contatto: asp@pec.aspbologna.it (di seguito anche "ASP"/"Azienda"/"Titolare"), ha disposto che al proprio interno venga osservato il presente Regolamento Interno per l'utilizzo delle risorse informatiche (di seguito "Regolamento"/"Documento") in ambito aziendale, intendendosi per "Risorse Informatiche" i sistemi, gli strumenti e le attrezzature informatiche e digitali di ASP.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete *Internet* da *personal computer*, *tablet* e *smartphone*, espone il Titolare e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla *privacy*, fra tutte), creando evidenti problemi alla sicurezza oltre che all'immagine del Titolare stesso.

Anche lo sviluppo delle reti sociali *on-line* incide, direttamente e/o indirettamente, sulle attività del Titolare e sulla sua immagine, costituendo, da un lato, un efficace strumento di condivisione di contenuti e altresì, al contempo, un rischio derivante dalla presenza della denominazione del Titolare e/o di altri riferimenti a esso riconducibili, eventualmente solo indiretta, sui *social media*.

Il presente documento, quindi, redatto a cura del Referente del D.P.O. (ossia il Soggetto *Sub*-Delegato Attuatore del Trattamento e Responsabile Servizio Risorse Umane) e del S.I., regolamenta l'accesso e il corretto uso delle risorse informatiche dell'ASP, secondo i principi e le disposizioni di legge in materia nel rispetto delle politiche e disposizioni aziendali, definite in accordo con la direzione di ASP.

In particolare le istruzioni riportate si rifanno alle normative in materia di:

- protezione dei Dati Personali
- crimini informatici
- disciplina dei rapporti di lavoro.

Il Documento opera nei confronti di chiunque, individuato come "Utilizzatore"/"Utente", si trovi a usufruire e servirsi del sistema informativo/Risorse Informatiche dell'Azienda quali:

- dipendenti di ASP
- collaboratori e consulenti
- terzi autorizzati a vario titolo

Scopo del Regolamento, pertanto, è quello di:

- agevolare la lettura e la comprensione del quadro normativo;
- fornire agli Utilizzatori le necessarie prescrizioni e istruzioni operative per un corretto e ottimale uso dei sistemi e delle attrezzature informatiche;
- scongiurare il rischio di un uso improprio (anche accidentale) o illecito delle Risorse Informatiche aziendali che costituirebbero un danno per ASP, reale o potenziale, quali:
  - → perdita di risorse (esempio: disponibilità/efficienza del sistema complessivo, tempo lavorativo del dipendente, disservizi *ecc.*);
  - → danni diretti (esempio: introduzione di virus, *data breach*, commissione di reati eventualmente attribuibili ad ASP *ecc.*)

Il Documento, pertanto, è di complemento al Codice di Comportamento Aziendale[4] anche in merito alla possibile attivazione di procedimenti disciplinari.

Quanto alle necessarie e opportune attività di controllo e vigilanza finalizzate esse:

- rispondono al principio della "proporzionalità" secondo i criteri di pertinenza e non eccedenza del controllo stesso;
- sono finalizzate esclusivamente a garantire la sicurezza del sistema informatico e l'appropriato utilizzo delle risorse: in particolare l'Azienda garantisce che i Dati informatizzati da essa gestiti,

[4] Disponibile al *link* Regolamenti-Disposizioni (aspbologna.it)

nonché i sistemi di elaborazione Dati e gli strumenti di telecomunicazioni, non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114, 171 Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300)[5].

Per le misure in materia di protezione dei Dati Personali, ma non esclusivamente relative al Trattamento di Dati con supporto informatico, si rinvia ad altra documentazione aziendale specifica.

3. Le principali definizioni[6]

Risorse Informatiche

Qualsiasi mezzo di comunicazione ed elaborazione elettronica, *hardware*, *software*, rete, servizio e informazione in formato elettronico di proprietà di ASP o in sua disponibilità o a essa concesso in licenza d'uso.

Le risorse informatiche includono a titolo di esempio:

- sistemi informatici a uso sociosanitario, amministrativo o tecnico (es. posta elettronica, accesso a *Internet*, applicativi Aziendali quali Cartella Ospiti, *Eusis*, *Domus*, Gestione risorse umane, Protocollo Informatico ecc.);
- ogni sottosistema di elaborazione elettronica delle informazioni: *server*, *personal computer* fissi o portatili, *tablet* e similari (inclusi *smartphone*);
- *software* di base e di ambiente: sistemi operativi, *software* di rete, sistemi per il controllo degli accessi, *package*, *utility* e similari;
- *software* di produttività individuale (*MS Office*, *LibreOffice*, *OpenOffice*, *Project*, *Visio* ecc.);
- ogni informazione elettronica registrata o conservata in file e banche Dati (es. CD, nastri, dischi esterni *ecc*.);
- ogni periferica: stampanti, *scanner*, *plotter*, apparecchiature per l'archiviazione elettronica dei Dati, supporti di memorizzazione, video terminali, lettori ottici;
- ogni dispositivo di rete: concentratori, ripetitori, *modem*, *switch*, *router*, *gateway*, *firewall*, apparati VoIP e similari, *access point*, chiavette *Internet*;
- ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche: cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, *patch* e similari.

Settore Informatico

Il Settore Informatico (S.I. nel seguito del documento) è costituito dall'insieme dei soggetti, dipendenti e collaboratori, che fanno capo all'Unità di *Staff,* collocata in seno alla Direzione Amministrativa di ASP Città di Bologna e denominata "*Information Technology*", la quale amministra, governa, sovraintende e presidia tutti gli aspetti relativi alla gestione delle Risorse Informatiche aziendali, anche in coordinamento e collaborazione con eventuali consulenti e collaboratori (es: il Responsabile per lo sviluppo dei sistemi informatici, gli amministratori di sistema *ecc.*). Essa costituisce il punto di riferimento, *in primis* tecnico:

→ per tutti gli Utenti (in relazione all'uso di dette Risorse Informatiche e ai relativi profili di sicurezza)

→ per tutti i fornitori esterni collegati, ai quali potranno essere impartire le direttive necessarie all'adempimento degli obblighi contrattuali sottesi in materia e ai correlati opportuni e necessari profili di sicurezza e ottimizzazione dell'interezza delle Risorse Informatiche.

In particolare il S.I. si farà carico, tra gli altri, di:

→ indirizzare, sovraintendere e controllare le attività svolte dai fornitori aziendali di cui alle Risorse Informatiche di ASP

→ gestire le richieste pervenute dagli Utenti, anche con rinvio ai referenti esterni di cui ai competenti fornitori.

[5] In caso contrario, per il futuro, tali controlli potranno essere effettuati esclusivamente:1) nei limiti di legge in generale (in particolare: ex Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 - *Jobs Act* e s.m.i.), 2) all'esito di accordo sindacale, 3) previa informativa ai dipendenti interessati.
[6] Vd. anche Modello Organizzativo in materia di Protezione dei Dati Personali

Utilizzatori/Operatori/Incaricati

Persone fisiche dipendenti o collaboratori o consulenti, o frequentatori, o universitari, o terzi che, a vario titolo, hanno accesso a strumenti informatici e/o telematici collegati alla rete e/o ai sistemi di ASP e che risultano abilitati all'utilizzo degli stessi mediante consegna di credenziali di abilitazione.

Trattamento dei Dati Personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati personali e/o a insiemi di Dati personali, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'alterazione, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione e/o qualsiasi altra forma di messa a disposizione, il raffronto e/o l'interconnessione, la limitazione, la cancellazione, la distruzione, il recupero, il ripristino.

Interessato Trattamento

La persona fisica cui si riferiscono i Dati personali.

In merito al tipo di Dati si distinguono:

Dato Personale:

Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero d'identificazione, Dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati Particolari (ossia particolari categorie di Dati Personali):

Dati Personali che rivelino l'origine etnica, le opinioni politiche, le convinzioni religiose e/o filosofiche e/o l'appartenenza sindacale, nonché Dati genetici, Dati biometrici intesi a identificare in modo univoco una persona fisica, Dati relativi alla salute e/o alla vita sessuale e/o all'orientamento sessuale della persona (già definiti "dati sensibili") oppure Dati Personali relativi alla sottoposizione dell'Interessato a condanne penali, misure interdittive, procedimenti giudiziari (già definiti "dati giudiziari"); da ultimo sono da richiamarsi anche i Dati relativi alla geocalizzazione e/o alle comunicazioni informatiche.

In merito ai soggetti che possono effettuare operazioni di Trattamento si distinguono:

Titolare del Trattamento:

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente e/o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati personali; nel nostro caso Titolare del Trattamento è ASP Città di Bologna –Azienda di Servizi alla Persona legalmente rappresentata dall'Amministratore Unico *pro-tempore*.

Il Titolare deve non solo conformare il Trattamento dei Dati da lui operato in base ai principi di cui al GDPR, ma anche prevedere e valutare il rischio tipico (o prevedibile) connesso all'attività di ASP e introdurre misure organizzative e di sicurezza per eliminare o ridurre tale rischio.

Soggetto Delegato Attuatore

La persona fisica interna all'Azienda che opera sotto l'autorità del Titolare e che, a tal fine, deve essere espressamente designata e delegata a compiti e funzioni in materia di Trattamento dei Dati Personali. In ASP Il Soggetto Delegato Attuatore viene individuato nella figura del Direttore Generale il quale quindi è, come per nomina e delega, tenuto a dare seguito agli adempimenti organizzativi interni alla struttura del Titolare, conferendo autorizzazioni e istruzioni *privacy* alle figure organizzative di vario livello e deve essere in grado di dimostrare che il Trattamento è effettuato conformemente al GDPR.

Soggetti *Sub*-Delegati Attuatori

Le persone fisiche individuate e designate dal Soggetto Delegato Attuatore che agiscono nel rispetto delle direttive impartite dal Titolare del Trattamento e/o dal predetto Soggetto Delegato Attuatore (nei confronti dei quali si trovano in rapporto di subordinazione) in adempimento alle prescrizioni loro indicate, in ordine alla natura, durata e finalità del Trattamento/i assegnato/i, delle categorie di

Dati oggetto di Trattamento, delle misure tecniche e organizzative adeguate e, in via generale, delle disposizioni contenute nel Regolamento. IN ASP corrispondono ai Dirigenti/Responsabili di Servizio-Area-Ufficio (a seconda del caso) come da Organigramma Aziendale in materia di protezione dei Dati Personali.

Responsabile del Trattamento

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo esterno all'Azienda che tratta Dati Personali in nome e per conto del Titolare del Trattamento nell'ambito della fornitura di beni e servizi.

Incaricato/i al Trattamento

La/e persona/e fisica/he espressamente designata/e al Trattamento dei Dati, a cui il Titolare del Trattamento, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, normalmente attraverso l'azione dei Soggetti *Sub*-Delegati Attuatori del Trattamento attribuisce specifici compiti e funzioni connessi al Trattamento di Dati Personali.

Comunicazione del Trattamento

Il dare conoscenza dei Dati Personali a uno e/o più soggetti determinati diversi dall'Interessato, dal rappresentante del Titolare nel territorio dell'Unione europea, dal Soggetto Delegato Attuatore, dal Responsabile e/o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate (ai sensi dell'articolo 2-quaterdecies) al Trattamento dei Dati personali sotto l'autorità diretta del Titolare e/o del Responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione e/o mediante interconnessione.

Diffusione del Dati Personali

Dare conoscenza dei Dati Personali a "soggetti indeterminati", in qualunque forma, anche mediante la loro messa a disposizione e/o consultazione.
Per "soggetti indeterminati" s'intendono soggetti non identificabili a priori.

Archivio dei Trattamenti

Qualsiasi insieme strutturato analogico e/o digitale di Dati Personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato e/o ripartito in modo funzionale (dislocazioni logiche) o geografico (dislocazioni fisiche).

Misure di sicurezza

Le misure tecniche e organizzative definite dal Titolare del Trattamento e adeguate al rischio insito nel Trattamento effettuato.
Spetta infatti al Titolare eseguire, per ogni Trattamento, una valutazione dei rischi connessi, ovvero la probabilità e la gravità del rischio che lo stesso può comportare per i diritti e le libertà degli interessati. La valutazione del rischio è determinata tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento.
Le misure di sicurezza possono essere di tre tipologie:

1. **tecniche**, cioè volte a proteggere le architetture di rete, gli applicativi e le banche Dati e la trasmissione dei Dati stessi (esempio: autenticazione informatica, uso delle *password*, sistema di autorizzazione e configurazione dei profili di accesso, *antivirus* e antispam, *backup*, pseudonimizzazione/anonimizzazione dei Dati, *ecc.*);
2. **fisiche**, cioè volte a proteggere le aree, i locali e gli archivi da accessi non autorizzati (esempio: armadi chiusi a chiave, controllo degli accessi con badge o altri sistemi di registrazione dei visitatori, vigilanza, *ecc.*);
3. **organizzative**, cioè individuate dal Titolare per l'assegnazione di compiti e responsabilità, per la costituzione di una cultura aziendale sulla tematica di protezione Dati, per garantire che i Trattamenti avvengano per finalità autorizzate e consentite (esempio: informativa e consenso, deleghe di funzioni, autorizzazioni a trattare i Dati, definizione dei termini di conservazione dei Dati, gestione *data breach*, formazione dei dipendenti).

Credenziali di autenticazione

Le credenziali di autenticazione sono le chiavi di accesso a strumenti informatici, procedure e dispositivi. La consegna delle stesse all'Utilizzatore risulta essere una misura di sicurezza tecnica e nel contempo consente di correlare univocamente l'Utilizzatore ai Dati e ai dispositivi informatici in uso.
La parola chiave (*password*) è la componente di una credenziale di autenticazione associata a una persona, e solo a questa nota, costituita da una sequenza di caratteri o altri Dati in forma elettronica, da mantenere riservata.

4. Oggetto e campo di applicazione

Le regole stabilite si riferiscono a tutte le risorse informatiche di ASP, incluso l'accesso a *Internet* e l'utilizzo della posta elettronica, sono applicate da tutti i soggetti (dipendenti di ASP senza distinzione di ruolo e/o livello, collaboratori e consulenti di ASP a prescindere dal rapporto contrattuale con la stessa intrattenuto) che le utilizzano e/o che vengano autorizzati a far uso di strumenti tecnologici del Titolare e/o perfino di accedere alla rete informatica aziendale e, pertanto, a eventuali Dati e informazioni ivi conservati e trattati: conseguentemente, le regole di seguito previste devono intendersi a carico tanto degli stessi (ferma restando la necessità che si dia opportuno conto del presente Regolamento) e hanno valenza per tutte le tipologie di Dati.

ASP fornisce gli strumenti informatici e telematici agli Utilizzatori confidando sul comune impegno affinché:

- siano sempre garantiti sia il loro corretto ed equilibrato utilizzo, sia la sicurezza e l'integrità del sistema informatico/informativo;
- non vengano pregiudicate e/o ostacolate le attività dei singoli e/o della collettività a causa di un uso inappropriato delle risorse disponibili da parte del singolo;
- non vengano perseguiti interessi privati in contrasto con quelli pubblici.

Tutti coloro che per ragioni di servizio devono avere accesso ai servizi informatici aziendali devono previamente essere stati autorizzati al Trattamento dei Dati da parte del Titolare o del Soggetto Delegato Attuatore o del Soggetto *Sub*-Delegato Attuatore, come demandati.

I Dati possono essere trattati limitatamente alle operazioni indispensabili per l'esercizio delle rispettive funzioni.

Oltre a quanto definito in questo documento si precisa che per le risorse informatiche messe a disposizione e/o date in uso ad ASP da altri soggetti valgono gli accordi e le condizioni contrattuali stipulate fra le parti, cui di volta in volta è necessario fare riferimento e comunque compatibili con il presente Regolamento.

5. I principi

Le Risorse Informatiche sono parte integrante del patrimonio di ASP e pertanto:

- devono essere utilizzate per gestire le attività Aziendali, secondo le finalità autorizzate e definite dalla direzione aziendale e inerenti alla propria mansione, nel rispetto dei principi d'integrità e riservatezza, minimizzazione, esattezza, limitazione della conservazione;
- devono essere rese disponibili solo alle persone autorizzate e nei limiti di quanto necessario allo svolgimento dell'attività;
- devono essere protette mediante misure tecniche e organizzative adeguate, in modo da garantire la sicurezza dei Dati Personali dal rischio di trattamenti non autorizzati e/o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

In conformità al GDPR (e ss. ev. mod. e int.), alla legge in generale e alla *Policy* Aziendale, i Dati Personali e gestionali, gestiti con risorse informatiche, sono trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (principio di «liceità, correttezza e trasparenza»); sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità (principio di «limitazione della finalità»); sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di «minimizzazione dei Dati»); sono

esatti e aggiornati (principio di «esattezza»); sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di «limitazione della conservazione»); sono trattati in maniera da garantire una loro adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati e/o illeciti e dalla perdita, dalla distruzione e/o dal danno accidentali (principio di «integrità e riservatezza»).

6. I divieti

Di seguito si richiamano i principali divieti da rispettare nell'utilizzo delle risorse informatiche di ASP.
In particolare è fatto divieto di:

- introdursi abusivamente nei sistemi informatici aziendali.
- procurare a sé e/o ad altri profitto e/o arrecare danni all'Azienda, procurandosi, riproducendo, diffondendo, e/o consegnando codici, parole chiave e/o altri mezzi idonei all'accesso ai sistemi informatici.
- riprodurre, duplicare e/o asportare, comunicare a terzi, diffondere i Dati di cui l'Azienda è Titolare del Trattamento.
- riprodurre e/o asportare documentazione di qualsiasi tipo classificata riservata, compresi progetti, schede, prospetti, se non per fini particolari dietro esplicita autorizzazione del Titolare dei relativi diritti (o di persona delegata).
- intercettare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici.
- distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici e/o i programmi e le informazioni e/o i Dati esistenti nei sistemi.
- riprodurre, duplicare e/o asportare programmi installati di cui l'Azienda è licenziataria e/o proprietaria.
- introdurre, installare, utilizzare programmi che non siano stati regolarmente acquistati, distribuiti e/o installati dalle preposte funzioni Aziendali.
- adottare comportamenti che mettano a rischio la sicurezza del sistema informatico/informativo, inclusi i Dati contenuti e/o che pregiudichino e/o ostacolino le attività della collettività degli utilizzatori.

La violazione di tali divieti è punita con sanzioni di natura sia amministrativa che penale.

A titolo di esempio, si elencano di seguito alcune figure di reato di natura informatica previste dal Codice Penale:

- Attentato a impianti informatici di pubblica utilità (art. 420);
- Falsificazione di documenti informatici (art. 491bis);
- Accesso abusivo a un sistema informativo o telematico (art. 615ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater);
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informativo (art. 615quinquies);
- Violazione di corrispondenza telematica (artt. 616-617sexies);
- Intercettazione di e-mail (art. 617quater);
- Danneggiamento di sistemi informatici e telematici (art. 635bis);
- Frode informatica ovvero alterazione dell'integrità di Dati allo scopo di procurarsi un ingiusto profitto (art. 640ter).

Inoltre il Codice *Privacy* prevede le seguenti autonome fattispecie di reati:

- Trattamento illecito di Dati (art. 167);
- Comunicazione o diffusione illecita *di Dati personali oggetto di Trattamento su larga scala* (art. 167-bis);

- Acquisizione fraudolenta di Dati personali oggetto di Trattamento su larga scala (art. 167-ter);
- Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168);
- Inosservanza di provvedimenti del Garante (art. 170);
- Violazioni sui controlli a distanza dei lavoratori e indagini sulle opinioni (art. 171).

Infine il GDPR prevede un rilevante e articolato apparato sanzionatorio agli Artt. 83 e 84, cui si rinvia.

7. Responsabilità

7.1. Procedure informatizzate autorizzate

Le procedure informatiche distribuite e gestite dal S.I. sono quelle individuate nell'*Allegato 1 - Elenco applicativi di base e specifici autorizzati* dal Titolare del Trattamento in coordinamento con il S.I., il quale fornisce consulenza e supporto in tale ambito, unitamente agli altri soggetti esperti e a ciò deputati come da Organigramma Aziendale di ASP in ambito di protezione dei Dati Personali.

Pertanto, tutti i soggetti sovraindicati, ciascuno secondo il proprio ambito di competenze e relativa responsabilità, sono deputati alla messa in opera delle misure di sicurezza e alla verifica-monitoraggio del rispetto della normativa e delle disposizioni aziendali, con riferimento ai i *server*, i *software* di base, le procedure applicative, le infrastrutture, i dispositivi della rete aziendale.

Sono invece a carico degli Utilizzatori (Soggetto Delegato Attuatore, Soggetti *Sub*-Delegati Attuatori e Incaricati al Trattamento), ciascuno per i rispettivi ambiti di competenza e responsabilità) il rispetto sia, nello specifico, delle misure di sicurezza, sia, più in generale, della normativa e delle disposizioni aziendali, in particolare questo Regolamento, per quanto riguarda le postazioni di lavoro (*Personal Computer*) e le attività svolte con esse.

L'*Allegato 1* di cui *supra* sarà costantemente aggiornato dal S.I. e sempre disponibile in *Intranet* aziendale.

L'interezza delle disposizioni Aziendali in materia sarà oggetto di pubblicazione *sull'Intranet* Aziendale oltre che sul Sito *Internet* di ASP.

7.2. *Data breach*

In ottemperanza all'obbligo sancito dal GDPR, viene introdotta una procedura per la gestione degli episodi di violazione di Dati Personali – c.d. *Data Breach* - e delle eventuali relative notifiche alla Autorità Garante per la protezione dei Dati personali, nonché alla comunicazione agli interessati come previsto all'Allegato C) alla Delibera di Approvazione del presente Regolamento.

Pertanto tutti gli Utilizzatori dei sistemi informatici e telematici aziendali che abbiano notizia o sospetto di una possibile violazione di Dati sono tenuti ad attivare la procedura aziendale prevista in materia, di cui all'Allegato c) al presente Documento[7].

7.3. Procedure informatizzate non gestite dal S.I.

Fermo restando il divieto di utilizzare qualsiasi risorsa informatica non autorizzata, se, per qualsiasi ragione (con particolare riferimento alla necessità di garantire transitoriamente l'operatività impropriamente basata su detto utilizzo), ne fosse consentito l'uso, l'organizzazione e la gestione delle misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, sono a carico del singolo Utente (Soggetto Delegato Attuatore, Soggetto *Sub*-Delegato Attuatore e/o Incaricato al Trattamento, a seconda del caso), che deve rivolgersi al S.I. per verificarne la corretta applicazione.

8. Sistemi di autenticazione e di autorizzazione

Il Soggetto Delegato Attuatore o il Soggetto Sub-Delegato Attuatore del Trattamento dovrà richiedere al S.I. l'attivazione della credenziale di autenticazione informatica per ciascun

[7] Vedi anche Violazione dei dati personali (Data Breach) - Garante Privacy

Operatore/Utente/Incaricato da lui previamente autorizzato al Trattamento, specificando a quali Dati e tipi di operazioni egli possa accedere in relazione ai compiti impartiti.
Il Trattamento di Dati Personali con strumenti elettronici è consentito infatti ai soli Utilizzatori autorizzati come sopra e dotati di credenziali di autenticazione, in genere costituite da *Nome Utente* (*username*) e *password*.

8.1. Credenziali di autenticazione (coppia username e *password*)

Le credenziali di autenticazione sono il presupposto necessario per l'utilizzo dei sistemi informatici messi a disposizione da ASP.

Tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale devono essere intestatari di un nome *username* all'interno del dominio di sicurezza aziendale e, se diverso, di un Utente di posta elettronica.

Il nome Utente è legato alla persona e unico all'interno di ASP (non possono esistere utenze anonime).

Anche i fornitori esterni che devono accedere ai sistemi Aziendali sono stati dotati di credenziali di accesso, assegnate su richiesta del Direttore dell'Esecuzione del Contratto (DEC).

Il dominio Aziendale

Le credenziali di dominio consentono l'attivazione della procedura di autenticazione che permette l'accesso all'infrastruttura informatica, a uno specifico Trattamento o a un insieme di Trattamenti.

8.2. Accesso agli applicativi Aziendali

Tutte le informazioni relative alle modalità di abilitazione agli applicativi Aziendali sono disponibili *sull'Intranet* aziendale o tramite il S.I.

8.3. Gestione delle credenziali

Le credenziali possono consistere:
- in un codice per l'identificazione dell'incaricato (nome Utente o *username*), associato a una parola chiave riservata conosciuta solamente dal medesimo (*password*);

oppure

- in un dispositivo d'autenticazione (per esempio una carta magnetica o *smart card*) o un applicativo su cellulare (*app*) in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave anche a uso temporaneo (OTP: *one time password*) – cosiddetti sistemi di autenticazione *a doppio fattore*;

Per l'accesso a particolari tipologie di Dati saranno introdotti ove necessario sistemi che richiedono l'autenticazione a doppio fattore.

Rientrano nelle due prime tipologie, secondo il livello di utilizzo, le credenziali di tipo SpID (Sistema Pubblico di Identità Digitale[8]).

Nel caso più frequente le credenziali sono costituite da *username* e *password*.

Lo u*sername* (o nome Utente) è di norma costituito da una combinazione sintetica dei dati anagrafici principali.

Lo *username* di posta è di norma costituito dall'identificativo *nome.cognome*.

I casi di uguaglianza sono gestiti con l'introduzione di caratteri distintivi o qualificatori secondo necessità.

Se l'Utilizzatore è un soggetto esterno, l'identificatore di posta sarà del tipo *nome.cognome.ext*.

Lo stesso *username* non potrà, neppure in tempi diversi, essere assegnato a incaricati diversi.

La *Password* (o parola chiave) è una parola segreta conosciuta solo dall'Utilizzatore. In coppia con lo *username*, permette di accedere alla procedura informatizzata utilizzata dal dipendente. A tutti gli

[8] https://www.agid.gov.it/it/piattaforme/spid

utenti del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della parola chiave; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile (e anzi doveroso!) sostituirla anche prima. La parola chiave non deve contenere riferimenti facilmente riconducibili all'Utilizzatore. A tal fine il sistema di cambio *Password online* verifica che siano rispettati alcuni requisiti minimi di sicurezza nella composizione della stessa.

La *password* è strettamente personale e per nessun motivo deve essere resa nota ad altri soggetti. La sua conoscenza da parte di estranei consentirebbe il Trattamento dei Dati per nome e per conto del possessore delle credenziali, con imputazione di eventuale uso improprio di apparecchiature, strumenti o servizi al Titolare della *password* che ha consentito l'accesso.

A ogni Utilizzatore è assegnata individualmente una credenziale (in rari casi più credenziali) per l'autenticazione ai sistemi aziendali.

Le credenziali vengono disattivate nel caso di non utilizzo per oltre 6 mesi.

Le credenziali vengono disattivate anche in caso di perdita della qualifica o della mansione in funzione della quale l'Utilizzatore era autorizzato ad accedere ai Dati personali.

Sono esplicitamente vietate credenziali di accesso anonime, ovvero non corrispondenti a una persona fisica.

La scelta sicura della *Password* si realizza attraverso le seguenti regole di buon senso:

- deve essere facilmente memorizzabile in modo tale che si possa evitare di doverla scrivere (in particolare è fatto esplicito divieto di scriverla sulla postazione di lavoro o in prossimità), ma non banale e di facile individuazione (per esempio con riferimenti chiari all'incaricato);
- la sua lunghezza deve essere di almeno otto caratteri e deve contenere almeno un numero e una lettera maiuscola[9];
- non deve contenere lo *username* assegnato alla persona;
- dev'essere modificata al primo utilizzo e successivamente ogni tre mesi (le regole saranno pre-impostate nei sistemi gestionali);
- deve essere modificata tempestivamente ogni volta che si abbia la sensazione che possa essere conosciuta, intenzionalmente o accidentalmente, da altri;
- in caso di modifica, la nuova *password* non deve essere uguale a una *password* già usata in precedenza.

Il cambio *password* può essere eseguito agevolmente dal sistema operativo *Windows*.

La *password* è strettamente personale: non va comunicata né consegnata né resa accessibile ad altro soggetto nello svolgimento delle attività aziendali, poiché tale azione espone il proprietario della stessa a responsabilità connesse all'utilizzo illecito è sanzionabile secondo quanto previsto nell'ambito della disciplina del Codice di comportamento dei pubblici dipendenti: pertanto dovrà essere custodita dall'Incaricato con la massima diligenza e non divulgata.

Non è consentita l'attivazione della *password* di accensione (bios), senza preventiva autorizzazione da parte del S.I.

Per completezza relativamente a una terza tipologia di credenziali, quella c.d. biometrica (ossia riferibile a una o più una caratteristica biometrica dell'incaricato -per esempio impronta digitale-, eventualmente associata a un codice identificativo e/ o a una parola chiave), si precisa che la stessa al momento non risulta in uso in ASP.

8.4. Sistema d'autorizzazione per le procedure informatizzate distribuite dal S.I.

L'assegnazione di credenziali di autenticazione abilita l'assegnatario all'utilizzo di una serie di strumenti di lavoro di base, quali a titolo di esempio:

- eventuale accesso a una casella di posta elettronica;

[9] Solo nel caso in cui, per es. per obsolescenza, lo strumento elettronico non consenta una *password* lunga 8 caratteri, questa deve avere lunghezza pari al numero di caratteri massimo consentito.

- visualizzazione del portale del dipendente;
- accesso a *Intranet*, *Extranet*, *Internet*.

L'abilitazione a tali strumenti di lavoro, ove non sia già stata assegnata d'ufficio, può essere richiesta al S.I. direttamente dall'Interessato.

Per l'abilitazione all'accesso a servizi informatici e procedure non comprese nei servizi di base, la relativa autorizzazione dovrà essere richiesta dal Soggetto *Sub*-Delegato Attuatore del Trattamento (o dal Soggetto Delegato Attuatore, secondo il caso) o cui afferisce l'Utilizzatore.
Previa autorizzazione da parte del Soggetto *Sub*-Delegato Attuatore del Trattamento (o dal Soggetto Delegato Attuatore, secondo il caso) saranno fornite, sempre attraverso il sistema informatizzato e senza ulteriori formalità, le credenziali di accesso richieste.

È dovere del Soggetto *Sub*-Delegato Attuatore del Trattamento (o dal Soggetto Delegato Attuatore, secondo il caso), che approva la richiesta informatizzata (o è firmatario della apposita modulistica ove presente), dare immediata comunicazione al S.I. circa la modifica o revoca di funzioni che avevano giustificato l'accesso da parte di un proprio collaboratore a procedure/banche Dati/servizi, conseguenti a dimissioni, trasferimenti, quiescenza del dipendente/Utilizzatore.

Salvo casi eccezionali, la richiesta di una nuova attivazione deve pervenire con almeno 10 giorni d'anticipo rispetto alla data di attivazione del codice identificativo.
Anche la richiesta di modifica di un profilo di abilitazione deve pervenire con almeno 10 giorni d'anticipo rispetto alla data di variazione.

La maggior parte dei servizi e procedure informatiche distribuite dal S.I. prevedono differenti profili di autorizzazione: tali profili, definibili per ciascun Utilizzatore o per classi omogenee di utilizzatori, devono essere individuati e configurati anteriormente all'inizio del Trattamento, in modo da limitare l'accesso ai soli Dati necessari per effettuare le operazioni di Trattamento.

Periodicamente, e comunque almeno annualmente, i Soggetti *Sub*-Delegati Attuatori del Trattamento (o il Soggetto Delegato Attuatore, secondo il caso) dovranno verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione attribuiti ai singoli Utilizzatori. Per semplificare tale attività il S.I. renderà periodicamente disponibili, anche su sistema informatizzato, gli elenchi degli Utenti con le abilitazioni e i profili assegnati, relativamente alle principali procedure informatiche aziendali.

8.5. Designazione Trattamento Dati Personali

Il soggetto abilitato con credenziali di autenticazione per l'utilizzo degli strumenti di lavoro che consentono l'ottenimento dei relativi servizi informatici, informato preventivamente in merito alle modalità di Trattamento dei Dati Personali che lo riguardano, deve essere designato al Trattamento dal Soggetto *Sub*-Delegato Attuatore del Trattamento (o dal Soggetto Delegato Attuatore, secondo il caso) secondo quanto stabilito dall'art. 2-quaterdecies del D.Lvo 101/2018.

9. Norme generali per l'utilizzo delle Risorse Informatiche

L'Utente deve utilizzare in modo corretto e lecito le risorse che gli sono state messe a disposizione.

All'Utente è consentito l'utilizzo degli strumenti informatici forniti dall'Azienda per poter assolvere alle proprie incombenze personali senza doversi allontanare dalla sede di servizio purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali

Si riportano di seguito alcune tra le principali indicazioni che tutti gli utilizzatori devono rispettare; il S.I. è a disposizione per fornire chiarimenti e ulteriori precisazioni in merito ad aspetti che possano risultare complessi o troppo tecnici.

9.1. *Computer* aziendali

Il *Personal Computer* ("*P.C.*") aziendale in dotazione è uno strumento di lavoro. Non è consentito alcun utilizzo personale e/o improprio dello stesso poiché un tanto potrebbe comportare inefficienze, minacce e/o problemi alla sicurezza e costi di manutenzione imprevedibili.

Il *P.C.* deve essere usato in condizioni di sicurezza e stabilità che lo preservino da pericoli di danneggiamento e/o deterioramento.

Possono essere utilizzati unicamente programmi/applicazioni installati e/o autorizzati dal SI e per i quali siano stati regolarmente assolti gli oneri relativi alla concessione delle licenze d'uso, ove richieste. In caso di necessità di ulteriori applicazioni il dipendente dovrà farne richiesta al S.I.

È vietato disinstallare e/o disattivare i *software* presenti sul *P.C.*, in particolare i sistemi di protezione e sicurezza aziendali (tra cui l'antivirus), e i prodotti *software* d'inventariazione e controllo remoto: eventuali eccezioni devono essere concordate con il S.I. ed esplicitamente autorizzate.

Il personale tecnico potrà effettuare verifiche automatizzate o puntuali sui *software* presenti nelle postazioni, rimuovendo o bloccando l'esecuzione dei *software* non autorizzati, richiedendo eventualmente giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

L'Utilizzatore è personalmente responsabile del *P.C.* assegnatogli; egli ha pertanto l'obbligo, per quanto nelle sue possibilità, di impedire ad altri indebiti utilizzi dell'apparecchiatura informatica.

Si sottolinea che il furto di un *computer* impatta fortemente, oltre che sotto il profilo patrimoniale, anche in relazione a un possibile improprio utilizzo dei Dati in esso contenuti e/o alla perdita degli stessi: qualora ciò avvenisse, è obbligatorio darne segnalazione tempestivamente all'Amministratore di Sistema e/o al S.I. e alla Direzione di ASP, anche al fine di dare seguito a eventuali segnalazioni obbligatorie di *Data Breach* alla Autorità Garante per la protezione dei Dati e/o all'Interessato come obbligatoriamente previsto dalla norma.

Per finalità di sicurezza e risparmio energetico, *P.C.* e *monitor* devono sempre essere spenti al termine del loro utilizzo. Le apparecchiature devono essere disattivate anche nel caso di prolungate assenze dal servizio, pur nell'ambito dell'orario di lavoro.
Fanno eccezione a questa regola gli strumenti utilizzati tramite accesso remoto per prestazioni di lavoro agile-*smart working* e/o telelavoro.

In caso di assenze brevi (esempio: pausa mensa, riunione, *ecc.*) durante le quali l'apparecchiatura rimane incustodita è obbligatoria l'attivazione dello *screensaver* (salvaschermo) protetto da *password*. Per i *P.C.* in dominio il salvaschermo è configurato centralmente.

Al *P.C.* possono essere connesse solamente periferiche e/o dispositivi forniti e/o autorizzati dall'Azienda, da utilizzarsi esclusivamente se necessari per le attività Aziendali.

Nessuna periferica e/o dispositivo componente la stazione di lavoro può essere rimossa, salvo specifica autorizzazione (per esempio: in caso di utilizzo temporaneo per lavoro agile-*smart working*).

Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del S.I. nel caso in cui siano rilevati *virus* e adottando quanto previsto dal presente Regolamento in materia.

Il personale tecnico del S.I. (o delegato) potrà effettuare verifiche automatizzate e/o puntuali sulle periferiche presenti nelle postazioni, disabilitando e/o rimuovendo le periferiche non autorizzate, eventualmente chiedendo motivazioni e giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

Il Titolare rende noto che il personale incaricato al S.I. è stato autorizzato a compiere interventi nel sistema informatico Aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (esempio: aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware*, *ecc.*). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Titolare, si applica anche in caso di assenza prolungata o impedimento dell'Utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il S.I. ne darà comunicazione agli Utenti interessati, preventivamente oppure, nel caso di urgenza dell'intervento stesso, successivamente a esso.

Il personale incaricato del S.I. ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni *P.C.* al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la

massima sicurezza contro *virus, spyware, malware*, *etc*. L'intervento viene effettuato esclusivamente su chiamata dell'Utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

9.2. *Computer* portatili aziendali

Oltre a quanto indicato nel paragrafo precedente, gli utilizzatori dei *P.C.* aziendali (includendo anche *tablet*, mini *P.C. ecc.*) devono seguire le ulteriori seguenti istruzioni.

Il *P.C.* portatile deve essere conservato con cura sia durante gli spostamenti sia sul luogo di utilizzo aziendale e/o *extra* aziendale. In particolare devono essere adottate idonee precauzioni per preservarlo da accessi non autorizzati, furti e/o effrazioni, custodendolo in luogo sicuro in caso di allontanamento, anche temporaneo.

Il *computer* portatile non può contenere Dati personali e/o sensibili di soggetti interessati. Nel caso questo fosse inevitabile, il S.I. provvederà, su richiesta esplicita e motivata, a dotare i portatili di ulteriori sistemi di sicurezza (es. crittografia dei contenuti, sistemi antifurto ecc.).

L'utilizzo nell'esercizio del lavoro agile-*smart working* come da Piano Integrato di Attività e Organizzazione di ASP (PIAO) sarà non solo consentito ma anche promosso e favorito mediante dotazione di strumenti aziendali adeguati.

9.3. Utilizzo di attrezzature informatiche personali

In via generale, per la resa della mansione da parte del Personale di ASP (né per altre ragioni), non è previsto l'impiego di attrezzature personali di qualsiasi tipologia (PC, *tablet*, *smartphone*, *ecc*.) come collegate alla rete Aziendale.

Tuttavia, qualora occorresse:

→ in casi eccezionali e di necessità;

→ su richiesta motivata al S.I. (presentata -a seconda dei casi- dall'interessato direttamente o tramite suo Soggetto Delegato Attuatore e che individuerà i servizi aziendali interessati da detto utilizzo);

→ previo conseguente rilascio di specifica autorizzazione scritta da parte del S.I. (che predisporrà e/o comunicherà all'Utilizzatore eventuali misure/accorgimenti in ambito di sicurezza opportune e ulteriori rispetto a quelle di cui al presente Regolamento);

i dispositivi personali potranno collegarsi, a sottoreti appositamente predisposte nel rispetto della sicurezza della rete Aziendale e pertanto destinate a funzioni limitate.

9.4. Stampanti, *scanner* e fotocopiatrici multifunzione

Salvo eccezioni particolari e giustificate (esempio: ambulatori, guardiole, sportelli, *ecc.*), indipendentemente dalla richiesta, saranno sempre installate stampanti di rete e/o fotocopiatrici multifunzione (con funzione di stampante e *scanner*), in modo da consentirne l'uso condiviso tra più uffici, settori, strutture, anche al fine di un razionale utilizzo delle risorse assegnate.

Sono distribuite esclusivamente stampanti bianco/nero, generalmente *laser*. Nel caso si ritenga indispensabile l'acquisto di una stampante a colori, per es. per uso clinico, la richiesta dovrà essere in forma scritta inoltrata al S.I., adeguatamente motivata e sottoscritta dal Responsabile del Servizio richiedente.

Il medesimo processo autorizzativo, con l'invio al servizio competente, è richiesto per la fornitura di fotocopiatrici dipartimentali. È responsabilità del sottoscrittore della richiesta, in questo caso, garantire la congruità tra lo strumento richiesto (esempio: in termini di capacità produttiva, di tipo e quantità di accessori *ecc*.) e la reale necessità operativa (numero di copie mensili, necessità di stampe A4, *ecc*.).

È consentita la stampa solo dei documenti strettamente necessari, mentre dovrà essere sempre privilegiato l'utilizzo di documenti informatici. In caso di stampa è importante ritirarla prontamente

dai vassoi delle stampanti comuni per evitare un involontario accesso indesiderato a Dati personali. Si raccomanda in particolare di indirizzare le stampe di documenti contenenti Dati di salute o giudiziari verso una stampante dedicata e collocata in un'area controllata.

È buona regola, inoltre, privilegiare la stampa di documenti in modalità fronte/retro e bianco/nero in "modalità risparmio".

In caso di necessità di stampa di documenti particolarmente lunghi o di un numero significativo di copie, si consiglia di valutare l'utilizzo di un Centro Stampa.

Nell'utilizzo dello *scanner* accertarsi di utilizzare sempre una bassa risoluzione di scansione (esempio: 300 dpi), in particolare prima di inviare, per esempio via *e-mail*, un documento scansionato.

Si ricorda che nel caso di utilizzo di *scanner* deve essere sempre rispettata la normativa sul diritto d'autore, analogamente a quanto avviene per la riproduzione di documenti attraverso fotocopiatrici.

Non possono essere scansionati documenti aventi contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, origine etnica, opinione e appartenenza sindacale e/o politica.

Si rinnova il divieto d'invio tramite stampanti di rete di messaggi di posta elettronica contenenti Dati di natura sensibile, quali i Dati di salute, anche in considerazione del mittente non identificabile. Fa eccezione solo l'invio a sé stessi: è opportuno pertanto, una volta effettuata la scansione del documento che s'intende spedire con la posta elettronica, inviarlo previamente alla propria casella *e-mail* e successivamente effettuare l'invio dell'*e-mail* dalla propria postazione e dal proprio *account* di posta, scegliendo il documento da tale cartella; il documento dovrà essere protetto da *password*.

9.5. Supporti di memorizzazione (*CD*, *DVD*, *hard disk* esterni, *memory card*, *pen drive*)

L'utilizzo di tutti i supporti digitali e magnetici esterni e rimovibili (quali, ad esempio: *hard disk* esterni, *CD*, *DVD*, *hard disk* esterni, *memory card*, *pen drive* ecc.) contenenti Dati Personali nonché informazioni costituenti *know-how* aziendale deve avvenire con molta cautela e solo per lo svolgimento delle attività aziendali onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto e/o perso a/o divulgato e/o, successivamente alla cancellazione, recuperato/ripristinato. Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica *antivirus*/*malware,* che non deve essere interrotta dall'Utente per permettere al sistema di sicurezza di completare la verifica. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, manovra che rischia di danneggiare e rendere non più leggibili i Dati presenti sul dispositivo: nel caso venga rilevato un *virus*, dovrà essere prontamente consegnato al personale del S.I.

È vietato l'uso di periferiche e supporti removibili per il salvataggio e la memorizzazione di Dati personali o appartenenti a particolari categorie, quali i Dati di salute. Infatti l'eventuale perdita accidentale del supporto, il cui contenuto non sia crittografato, consentirebbe a chiunque di accedere ai medesimi Dati, configurando un'ipotesi di *data breach* da segnalare all'Autorità Garante per la protezione dei Dati e/o all'interessato.

Nel caso fosse strettamente necessario (ad esempio nel caso in cui il dispositivo sia utilizzato per le copie di sicurezza) è obbligatorio criptare i Dati con programmi adeguati, in genere già contenuti negli stessi supporti: per eventuali istruzioni rivolgersi al personale tecnico del S.I.

È vietato l'utilizzo di supporti rimovibili personali, salva autorizzazione al Dipendente del Soggetto *Sub*-Delegato Attuatore del Trattamento e solo per opportunità di servizio.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza e/o per trasportare *file* di grandi dimensioni, rimane in ogni caso sotto l'esclusiva responsabilità dell'Utilizzatore e deve essere effettuato avendo cura di cifrare i Dati Aziendali riservati e i Dati Personali o sensibili con l'utilizzo di *password* sicure.

Alcune raccomandazioni di buon senso:

- i supporti rimovibili (*CD*, *DVD*, *pen drive, memorie flash* per macchine fotografiche digitali e palmari, *hard disk* rimovibili, *ecc*.) devono essere custoditi con la massima riservatezza e con la massima

diligenza e non devono essere lasciati incustoditi o facilmente accessibili da parte di altri incaricati non autorizzati al Trattamento dei Dati contenuti;

- in particolare, durante il loro utilizzo devono essere presidiati dagli Incaricati e quando non temporaneamente utilizzati devono essere riposti in contenitori sicuri;
- i supporti rimovibili possono essere utilizzati e ceduti solamente tra le persone autorizzate al Trattamento dei Dati in essi contenuti;
- i supporti rimovibili non riscrivibili, per i quali i Dati presenti non possono essere eliminati attraverso procedure di formattazione del supporto (esempio: *CD-R*, *DVD-R*, *DVD+R*, *ecc*.), devono essere distrutti fisicamente nel momento in cui si ritiene non debbano essere più utilizzati per il Trattamento. In caso d'impossibilità o di difficoltà nell'esecuzione di quest'operazione rivolgersi al S.I. per la distruzione e lo smaltimento;
- i supporti rimovibili riscrivibili (esempio: *CD-RW*, *DVD-RW*, *DVD+RW, pen drive*, memorie *flash* per macchine fotografiche digitali e palmari, *hard disk* rimovibili, *ecc*.) non più utilizzati per il Trattamento di Dati devono essere formattati completamente (utilizzando appositi *software* o impostando opportuni parametri in fase di formattazione) da parte degli utilizzatori, in modo che i Dati precedentemente in essi contenuti non siano intelligibili e non siano tecnicamente in alcun modo ricostruibili: qualora ciò non fosse tecnicamente possibile, al pari dei supporti non riscrivibili devono essere distrutti; in caso d'impossibilità o di difficoltà nell'esecuzione di quest'operazione rivolgersi al S.I. per la distruzione e lo smaltimento.

È vietato consegnare a terzi supporti in precedenza utilizzati per la memorizzazione di Dati personali di natura sensibile, anche se apparentemente cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo la cancellazione.

L'Utente/Incaricato al Trattamento è tenuto a comunicare immediatamente al proprio Soggetto *Sub*-Delegato Attuatore[10] e a denunciare all'autorità giudiziaria l'eventuale furto, lo smarrimento, la perdita e/o l'appropriazione a qualsivoglia titolo da parte di terzi dei supporti rimovibili.

9.6. Norme generali per l'utilizzo del *software* distribuito dal S.I.

L'Utilizzatore autorizzato al Trattamento mediante *software* applicativi Aziendali:

- deve utilizzare il *software* solo per attività Aziendali;
- deve custodire il *software* ricevuto in dotazione;
- non deve cedere il *software* a colleghi o a terzi;
- deve utilizzare solo il *software* Aziendale assegnato.

Inoltre si ribadisce che:

- è vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), traduzione, distribuzione di *software* di terzi, che non sia autorizzata in base alla licenza a esso applicabile;
- salvo specifiche autorizzazioni, non è consentito l'uso in Azienda di *software* acquisito privatamente o disponibile gratuitamente, né l'uso all'esterno di ASP di *software* Aziendale;
- è vietato all'Utente che disponga dei diritti per farlo, alterare le impostazioni del sistema operativo o degli applicativi in senso contrario ai criteri minimi di sicurezza (in particolare a quanto indicato dalle circolari AgID del 2017 es. attivazione dell'esecuzione automatica di macro nei *file* di office, visualizzazione automatica del contenuto dei *file* ecc.).
- è vietato l'uso di programmi diversi da quelli ufficialmente installati dal personale del S.I. per conto del Titolare né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza delle presenti disposizioni espone il Titolare a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul *software* (che impone la presenza nel sistema di *software* regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore) vengono sanzionate penalmente e possono anche comportare il sorgere di una

[10] Individuabile come da Organigramma Aziendale in materia di Protezione del Dati Personali (All.C)

responsabilità amministrativa a carico del il Titolare, come disposta dall'art. 25-nonies del D.Lgs. 8 giugno 2001, n. 231 ed ev. ss. mod. e int., con applicazione di sanzioni pecuniarie e interdittive.

9.7. *Software antivirus* e di protezione dei Dati

Il S.I., mediante l'utilizzo di firewall e prodotti *antivirus* gestiti e aggiornati centralmente, assicura, nei limiti della tecnologia disponibile, la protezione dell'infrastruttura, dei sistemi informatici e delle postazioni di cui effettua la manutenzione.

L'aggiornamento dell'*antivirus* avviene giornalmente, quello delle *patch* critiche e di sicurezza di Windows avviene almeno mensilmente, previa verifica di consistenza e sostenibilità.

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico Aziendale mediante *virus* o mediante ogni altro *software* aggressivo.

È vietato il collegamento alla rete aziendale di qualsiasi *P.C.* non adeguatamente protetto mediante *software antivirus* (aggiornamento almeno settimanale) e *patch* di sicurezza del sistema operativo (aggiornamento almeno mensile).

In seguito alle indicazioni AgID, i sistemi aziendali saranno gradualmente impostati in modo tale che sia impedita la visualizzazione automatica del contenuto (per es. di un'*e-mail*), in particolare dei *file* allegati (per esempio la visualizzazione di un pdf in un'*e-mail*); così come continua a essere inibita l'esecuzione automatica da qualsiasi supporto (chiavette *usb*, *CD*, *DVD*, *ecc.*).

9.8. Dischi di rete, cartelle personali e cartelle condivise

L'Azienda mette a disposizione degli utilizzatori spazio su dischi di rete (cartelle che possono essere personali o condivise) per l'archiviazione d'informazioni di carattere professionale e aziendale.

Il sistema di salvataggio dei dati e delle informazioni aziendali in cartelle di rete deve considerarsi prioritario e preferibile rispetto al c.d. "salvataggio in locale"[11]: tutti gli utilizzatori, pertanto, sono inviatati a salvare i propri *file* aziendali sulle cartelle di rete in via preferenziale, permanendo l'opzione del salvataggio locale, come residuale e in via di dismissione.

Non possono essere collocati sulle unità di rete - nemmeno per periodi brevi - *file* personali o comunque aventi contenuto diverso da quello strettamente connesso all'attività lavorativa.

Vedi anche, più avanti nel documento, la possibilità di utilizzo del servizio *cloud* aziendale.

Il S.I. svolgerà periodici controlli a campione sulle unità di rete e può procedere autonomamente alla rimozione di Dati non connessi alle attività proprie di ASP. Nel caso in cui la natura o il contenuto di informazioni/Dati da collocare in rete per un utilizzo professionale potesse risultare dubbia/ambigua il Titolare o suo Delegato degli stessi dovrà informare preventivamente il S.I. affinché non proceda alla rimozione.

Il S.I. provvede al *backup* dei Dati collocati su unità di rete (completo mensile con *retention* di un anno, incrementale giornaliero con *retention* di 30 giorni). Nel caso di perdita di Dati in rete, pertanto, sarà possibile richiedere il recupero del *file* così come salvato nell'ultima versione di *backup*. Per questi motivi è fortemente consigliato l'utilizzo delle unità di rete per il salvataggio di Dati/*file* di particolare importanza e rilevanza.

Le unità di rete devono essere mantenute con diligenza a cura degli Utilizzatori; agli stessi è richiesta la periodica – almeno semestrale – revisione dei Dati salvati e l'eliminazione di quelli obsoleti o, comunque, non più utilizzati o necessari. È opportuno evitare la duplicazione di Dati per consentire uno sfruttamento razionale delle unità di rete.

È possibile che, per ragioni di razionalizzazione delle Risorse Informatiche, il S.I. introduca la limitazione degli spazi concessi a ciascun Utilizzatore e/o gruppi di utilizzatori in quote (esempio: 1GB, 5 GB, 10 GB) secondo la reale necessità di utilizzo delle Risorse Informatiche condivise.

[11] Metodologia di salvataggio di *file* che ne comporta la duplicazione e conservazione su un dispositivo presente fisicamente in Azienda (*hard disk* e *file server* locali).

I *server* aziendali centralizzati sono le uniche entità predisposte alla condivisione di risorse. È vietato condividere localmente e direttamente dischi, cartelle e/o risorse (es. cartelle di scambio) a eccezione delle stampanti comuni.

Fanno eccezione gli spazi messi a disposizione dalla piattaforma *cloud* la cui capienza è legata al tipo di licenza.

Solo in situazioni di particolari problematiche tecniche, su autorizzazione del S.I., potranno essere attivate condivisioni fra *personal computer* che dovranno inderogabilmente essere protette da *password* di accesso.

Per ogni cartella condivisa[12] il Soggetto *Sub*-Delegato Attuatore del Trattamento svolge la funzione di referente, avente la responsabilità di definire l'elenco degli Utilizzatori e dei profili di abilitazione, nonché di verificare il corretto utilizzo della cartella da parte degli utilizzatori stessi.

Al referente spetta verificare periodicamente e comunque almeno annualmente, le abilitazioni assegnate agli Utilizzatori, segnalando tempestivamente al S.I. la necessità di assegnare, modificare o cancellare l'accesso alla cartella da parte degli utilizzatori.

Lo spazio assegnato può essere concordato di volta in volta secondo le reali necessità.

10. Collegamento di attrezzature alla rete Dati

La rete dati aziendale su cavo o *wireless* (*wi-fi*) è gestita dal S.I.

L'accesso al *P.C.* e/o altre attrezzature alla rete aziendale dev'essere autorizzato dal S.I., che definisce la connettività da assegnare in base alle caratteristiche dell'attrezzatura e alle esigenze dell'Utilizzatore.

10.1 Rete di ASP

La rete interna permette l'accesso a tutti i principali applicativi aziendali e pertanto è destinata all'uso da parte dell'Utente aziendale esclusivamente mediante dispositivi di ASP.

Il collegamento alla rete di attrezzature informatiche personali, se ammesso, è regolato mediante accesso a sottoreti predisposte *ad hoc*.

Pertanto sono vietati:

- il collegamento alla rete aziendale di *P.C.* e *server* se non forniti o autorizzati dal S.I.;
- il collegamento alla rete aziendale di *P.C.* non adeguatamente protetti mediante *software antivirus* (aggiornamento almeno settimanale) e *patch* di sicurezza del sistema operativo (aggiornamento almeno mensile);
- il collegamento alla rete, non autorizzato dal S.I., di apparati di rete quali *switch*, *router* (anche *USB* o *wifi*) e attrezzature per reti *wireless* (esempio: *access point*);
- qualsivoglia forma di collegamento ad altre reti laddove la stazione di lavoro sia connessa alla rete di ASP.; conseguentemente:
  - ⇾ per le stazioni di lavoro connesse alla rete aziendale, sono vietate le connessioni tramite *modem* o chiavette *Internet* e l'utilizzo di una doppia scheda di rete;
  - ⇾ per i *P.C.* portatili dotati sia di scheda di rete tradizionale che di scheda di rete *wireless*, entrambe le schede possono essere abilitate al collegamento alla rete aziendale purché non vengano utilizzate contemporaneamente.

Le regole valgono anche per le attrezzature collegate e/o ospitanti strumentazioni medicali e analitiche.

[12] Per ogni Servizio/U.O. come da Organigramma Aziendale in materia di Protezione dei Dati Personali (All.C)

10.2. Altre reti *Wi-Fi* in ASP

Allo stato attuale non ci sono altre reti autorizzate dal S.I. oltre alla rete con SSID *emiliaromagnawifi*, fornita da Lepida, attivata per fornire servizi agli ospiti e agli accompagnatori sulle reti *WiFi* nelle strutture di ASP.

11. Uso e salvataggio dei Dati Aziendali (*backup*)

Il S.I. provvede al salvataggio dei Dati registrati tramite i sistemi informativi aziendali centralizzati.

La politica di *backup* (creazione di copie di sicurezza) definisce la frequenza di salvataggio e il tempo di tenuta dei *backup* e viene adottata dal S.I. in linea con indicazioni normative, raccomandazioni e *best practice*.

Al fine di salvaguardare tutti gli altri documenti aziendali ritenuti d'interesse e utilità per ASP (esempio: documenti *doc*, *xls*, *pdf ecc.*), è opportuno non memorizzarli sull'*hard disk* dei *P.C.*: a tale scopo dovranno invece essere utilizzati i dischi di rete e i server gestiti dal S.I.

Nel caso invece sia indispensabile memorizzare Dati Aziendali localmente sugli *hard disk* dei *P.C.,* è fatto obbligo agli utenti di effettuare una copia di sicurezza di tali Dati, con frequenza almeno settimanale e di procedere a crittografia degli stessi nel caso si tratti di Dati che richiedono la tutela della riservatezza.

Il S.I. a questo scopo fornisce, su richiesta, i dispositivi *hardware* necessari per il salvataggio dei Dati su supporto rimovibile. È fondamentale che tali supporti non siano permanentemente accessibili dal *P.C.* onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza: a tal fine si raccomanda di collegare i dispositivi di *backup* solo per il tempo strettamente necessario alla realizzazione della copia di sicurezza, rimuovendoli opportunamente al termine della copia e riponendoli in luogo sicuro (sul punto vedasi anche il successivo paragrafo 11.1).

11.1. Supporti di memorizzazione (CD, DVD, hard *disk* esterni, memory *card*, pen *drive*.)

È responsabilità degli Utenti conservare adeguatamente e proteggere le copie di *backup*.

Su richiesta saranno fornite dal S.I. istruzioni operative e strumenti per la crittografia dei *file*.

12. Utilizzo della posta elettronica

12.1. Definizioni e strumenti

Casella di Posta e *account*

Spazio dedicato alla gestione dei messaggi di posta in transito tra un qualsiasi Mittente e il Destinatario/Mittente proprietario della casella stessa. Si definisce "*account*" di posta l'identificativo dell'Utente necessario per essere riconosciuto come Utente unico dal servizio di posta elettronica. A ogni *account* è associata una parola chiave (*password*) nota soltanto all'Utente e sottoposta a regolamentazione. La *password* e *l'account* associati costituiscono la credenziale di autenticazione con la quale l'Utente può accedere alla propria casella di posta.

La *password* è strettamente personale e per nessun motivo deve essere resa nota ad altri soggetti: pertanto dovrà essere custodita dal Titolare con la massima diligenza che dovrà astenersi dal divulgarla e/o renderla accessibile ad altro soggetto in quanto la sua conoscenza da parte di estranei esporrebbe l'assegnatario della stessa a responsabilità connesse all'utilizzo illecito e/o improprio, sanzionabile secondo quanto previsto dal Codice Disciplinare e dalla normativa applicabile in generale.

Casella di Posta PEC

La posta elettronica certificata o PEC è un tipo particolare di posta elettronica che consente di attribuire a un messaggio di posta elettronica lo stesso valore legale di una tradizionale raccomandata con avviso di ricevimento, garantendone la prova dell'invio e della consegna. Ogni ente pubblico è dotato di una casella PEC istituzionale, chiamata PEI. Essa è inserita, eventualmente assieme a altre PEC Aziendali, in un elenco pubblico (chiamato IPA – Indice delle Pubbliche Amministrazioni, gestito

da AgID) e può essere utilizzata da un qualsiasi soggetto, pubblico o privato, che intenda inviare una comunicazione informatica valida agli effetti di legge all'ente intestatario della casella.

Il gestore del sistema di posta certificata di ASP Città di Bologna è un *provider* esterno qualificato: il dominio gestito è *@pec.aspbologna.it*, l'indirizzo della PEI è *asp@pec.aspbologna.it*.

Questa casella è sempre presidiata e integrata con il sistema di protocollo Aziendale.

Possono inoltre essere attivate altre caselle PEC pubbliche diverse dalla PEI, per i Servizi aziendali che ne dovessero richiedere l'utilizzo, e il cui elenco aggiornato sarà sempre riportato, ove necessario, nell'Indice delle Pubbliche Amministrazioni.

Casella di Posta aziendale individuale

Casella di posta elettronica associata a ciascun dipendente o collaboratore fornita d'ufficio o in seguito a sua richiesta. Ai dipendenti dotati di una postazione di lavoro individuale viene di norma assegnata d'ufficio una casella *e-mail* individuale secondo necessità e in accordo con le mansioni assegnate; inoltre l'*e-mail* Aziendale può essere fornita anche a soggetti non dipendenti, ma con altri rapporti di collaborazione con ASP, mediante apposita modulistica o su sistema informatizzato.

Per i soggetti esterni legati da relazioni commerciali (es. i fornitori di servizi) si utilizza un suffisso identificativo ".ext", in modo tale da rendere sempre nota la circostanza. L'indirizzo di posta apparirà nella forma *nome.cognome.ext@aspbologna.it*[13].

La casella di posta ordinaria è genericamente nel formato *nome.cognome@aspbologna.it*: i casi di uguaglianza sono gestiti con l'introduzione di caratteri distintivi o altre modalità secondo i casi.

Con la consegna della casella *e-mail* individuale viene anche fornita specifica informativa sul Trattamento Dati personali ex art. 13 del GDPR.

Valgono le disposizioni di cui al precedente *sub* "*Casella di Posta e account*".

Mailing list

È concettualmente equivalente all'*alias*[14], ma, in primo luogo ne supera i limiti imposti: si pensi agli elenchi di grandi dimensioni legati da:

- un particolare obiettivo pratico gestionale (come per esempio l'elenco degli indirizzi *e-mail* di tutti i dipendenti dell'Azienda, l'elenco dei Direttori di Struttura *ecc.*);

oppure

- un interesse comune (come per esempio gli utilizzatori di un determinato servizio, gli appassionati di un particolare tema *ecc.*).

Nel primo caso le liste sono costituite centralmente (*top down*), nel secondo caso si costituiscono mediante iscrizione degli interessati (*bottom up*).

Va precisato che gli indirizzi cui è associata una *mailing list*, anche se noti, non possono essere utilizzati da chiunque come un normale indirizzo *e-mail*, ma sono gestiti esclusivamente da personale autorizzato del S.I. (oppure gestito da specifica struttura indicata dalla Direzione Aziendale[15]) a cui è necessario rivolgersi per ogni utilizzo.

Casella di gruppo e casella delegata

Casella di posta elettronica associata a un nodo dell'organigramma aziendale o a un elemento funzionale dell'organizzazione aziendale: in questo caso la denominazione deve essere indicativa della funzione assegnata, mentre l'accesso per la consultazione e l'utilizzo avviene mediante gli *account* individuali della/e persona/e individuate dal Referente della funzione della struttura cui si riferisce la casella.

A tal proposito si precisa che nel caso la casella delegata sia utilizzata per comunicazioni con il cittadino, la funzione di visualizzazione del mittente delegato deve essere disattivata su esplicita

[13] salvo eccezioni presenti per ragioni storiche che saranno nel tempo eliminate
[14] Un *alias* di posta elettronica costituisce un re-indirizzamento a una casella di posta elettronica reale: in pratica sul *server* di posta elettronica viene creato un unico contenitore per l'Utente, ma al suo interno poi vengono create delle sottocartelle, ciascuna per ogni alias di posta elettronica creato.
[15] direzione@aspbologna.it

richiesta del Soggetto *Sub*-Delegato Attuatore del Trattamento (o il Soggetto Delegato Attuatore, secondo il caso) che si attiva per garantire la tracciabilità del soggetto che ha predisposto la corrispondenza (indicando per esempio: il numero di matricola e altra codifica opportuna).

La differenza rispetto all'*alias* è evidente, in quanto:

→ un'*e-mail* inviata a un *alias* raggiunge tutti i destinatari che la compongono;
→ un'*e-mail* inviata a una casella di gruppo raggiunge tale casella che è accessibile indifferentemente a tutti i componenti del gruppo (tramite *client* di posta configurato opportunamente).

È importante distinguere bene queste due tipologie quando se ne richiede la creazione; in linea di massima:

→ si predilige la casella di gruppo quando la posta deve essere "processata" internamente (per esempio perché dà avvio a un processo interno che richiede una risposta certa e risulta quindi fondamentale che tutti i componenti del gruppo abbiano visibilità di tale Trattamento, vedano le risposte, *ecc.*);
→ la *mailing-list* è invece ideale quando lo scopo primario è quello di condividere informazioni, quindi essere certi che tutti i componenti (per esempio di un gruppo di lavoro) ricevano le stesse *e-mail*.

La *casella delegata* si comporta come una casella di gruppo, ma è fittizia e funziona esclusivamente per delega: va utilizzata quando non è necessario disporre di una vera e propria casella di organigramma, ma è sufficiente condividere l'utilizzo tra colleghi (per esempio di una segreteria).

Casella anonima

Si tratta di una casella tipicamente associata a un nodo dell'organigramma, alla quale tuttavia non è associato alcun nominativo reale e che può essere utilizzata da un gruppo di persone per condividere risorse: questo tipo di caselle mail è vietato in ASP e non sono quindi presenti.

Casella privata

Casella di posta elettronica fornita da *provider* estranei all'ambito aziendale (esempio: @gmail.it, @virgilio.it, @libero.it, @fastwebnet.it ecc.): come già rilevato queste caselle non dovrebbero mai essere inserite in un *alias*.

Sistema di protocollo informatico e messaggistica interna

Sistema utilizzato da ASP per la gestione della documentazione amministrativa, costituito pertanto da tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali. Il sistema di protocollo[16] include anch'esso un sistema di messaggistica strettamente integrato nella sua funzionalità, che consente la gestione di flussi documentali e la comunicazione a essi associata, nonché l'inoltro dei documenti per competenza o coinvolgimento. È importante pertanto che tutte le operazioni che possono essere effettuate con i sistemi documentali (protocollo, decisioni, delibere) non siano inutilmente replicate mediante il sistema di posta elettronica.

***Webmail* e altri programmi *client* di posta**

L'accesso a una casella di posta aziendale e alla corrispondente gestione delle proprie *e-mail* (ricezione, invio, modifica, inoltro ecc.) deve avvenire attraverso l'uso dello strumento fornito dal S.I.

12.2. Attribuzione della casella personale di posta elettronica aziendale

L'utilizzo della casella di posta elettronica costituisce, nei casi sovraindicati, un diritto e un dovere per ogni dipendente: pertanto, se non sussistono giustificati impedimenti, essa gli viene assegnata d'ufficio. L'intestatario della casella è responsabile della lettura e dell'invio dei messaggi, ed è responsabile della custodia e dell'aggiornamento della *password* di accesso esclusiva.

[16] Lapis di Zucchetti

12.3. Utilizzo della posta elettronica aziendale

La casella di posta aziendale (usualmente nella forma *nome.cognome@aspbologna.it*), sia essa individuale o di gruppo (condivisa), è uno strumento di lavoro che ha tanto lo scopo di inviare/ricevere comunicazioni direttamente attinenti alla propria attività lavorativa, quanto quello di ricevere comunicazioni/informazioni riguardanti ASP e/o il proprio rapporto di lavoro e non può in alcun modo compromettere la sicurezza e/o la reputazione di ASP e/o della Pubblica Amministrazione in generale.

Conseguentemente ciascun assegnatario di casella *e-mail* è pertanto direttamente responsabile del suo corretto utilizzo e quindi del contenuto dei messaggi inviati e si uniforma alle modalità di firma degli stessi come individuate da ASP per ciascun servizio di appartenenza: invero, ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare il recapito istituzionale al quale lo stesso è reperibile.

Per queste funzioni non è ammesso l'utilizzo di caselle di posta private (esempio: @virgilio.it, @libero.it, @gmail.it *ecc.*), che è quindi di norma escluso per attività e/o comunicazioni afferenti il servizio, fatti salvi i casi di forza maggiore relativi all'impossibilità per il dipendente, per qualsivoglia ragione, di accesso all'*account* aziendale.

È fatto salvo l'utilizzo della casella di posta personale per la ricezione di comunicazioni aziendali, come da opzione indicata dal dipendente in sede di assunzione.

È vietato l'invio di messaggi di posta elettronica, all'interno e all'esterno dell'Azienda, che siano oltraggiosi e/o discriminatori e/o che possano essere in qualunque modo fonte di responsabilità per ASP.

Di norma non è considerato opportuno l'utilizzo della posta elettronica aziendale, anche se l'*account* è individuale, per motivi diversi da quelli strettamente legati all'attività lavorativa e quindi per scambiare comunicazioni e/o svolgere attività che non rientrino tra i compiti istituzionali, fatto salvo quanto previsto dalla precedente clausola *sub*. 9.

12.4. Attribuzione della casella PEC

La casella PEC può essere integrata nell'applicativo di gestione documentale per l'utilizzo nel sistema di protocollo Aziendale o utilizzata per la corrispondenza che richieda particolari garanzie in merito all'invio e alla consegna[17].

La PEC viene attribuita esclusivamente alla struttura di afferenza.

Non vengono assegnate caselle PEC nominative ai professionisti, in quanto fornite dai rispettivi Albi.

Nel caso in cui una sola persona sia abilitata all'accesso alla casella di struttura si parla di casella monoutenza; qualora invece la casella di struttura è multiutenza più persone possono essere abilitate all'accesso mediante credenziali personali.

12.5. La tutela della riservatezza

Come per tutte le informazioni attinenti all'attività lavorativa è vietata la divulgazione, per fini estranei alla stessa, d'informazioni e Dati ricavati/elaborati da procedure/banche dati aziendali e/o documenti, anche istruttori di cui abbiano disponibilità.

Inoltre, come noto, la comunicazione e la diffusione non autorizzata di Dati Personali costituiscono una grave violazione della normativa in materia: l'Azienda provvederà a configurare i singoli *account* al fine di inserire il c.d. discalimer nei messaggi in uscita dall'Azienda.

12.6. Invio tramite *e-mail* di documentazione sanitaria

L'invio tramite posta elettronica ordinaria (*e-mail*) di documentazione sanitaria (e, più in generale, di Dati Personali) è vietato fatti salvi i casi di ricezione/invio:

⇒ tramite PEC

[17] Vedi Codice dell'Amministrazione Digitale all'Art. 48

oppure

⇒ con l'impiego di procedura di cifratura secondo le indicazioni fornite, a richiesta, dal S.I.

12.7. Le regole di buon comportamento per l'utilizzo delle caselle *e-mail*.

L'utilizzo della posta elettronica è un dovere oltre che un diritto dell'Utilizzatore assegnatario.
Di seguito si riportano alcune indicazioni e regole di buon senso cui l'Utente deve attenersi nell'utilizzo dei sistemi di comunicazione.

a) Controllare la posta ogni giorno, eventualmente cancellandola dalla propria casella se non è necessario conservarla[18], prestando particolare attenzione alla rimozione degli allegati "pesanti". Infatti secondo il tipo di casella sussistono dei limiti dello spazio disponibile, eventualmente ampliabile in caso di necessità. In ogni caso la conservazione dei soli messaggi di interesse semplifica la consultazione e rende più efficienti le ricerche dei messaggi. A tal fine è consigliata l'articolazione delle cartelle di posta elettronica in sottocartelle e la classificazione con *tag* in modo da ottimizzarne la ricerca.

b) Controllare a ogni invio la correttezza degli indirizzi cui si scrive soprattutto se in modo aggregato e automatico.

c) Valutare con la massima attenzione e con razionalità il contenuto dei messaggi evitando di cadere in truffe o altri abusi: invero, nonostante i sistemi di controllo centrali permettano di bloccare la maggior parte dei messaggi potenzialmente pericolosi, alcuni messaggi oggetto di *spam*[19] o *phishing*[20] o contenenti *virus* possono eludere tali sistemi, pertanto l'attenzione di chi li riceve è sempre indispensabile al fine di evitare spiacevoli o pericolose conseguenze quali diffusione di informazioni personali o sensibili o persino blocchi del sistema e perdita di Dati.

d) Il personale del S.I. non chiederà mai a un Utente di inserire la propria *password* in un modulo raggiungibile da un collegamento via *e-mail*: pertanto qualora venisse rivolta questa richiesta all'Utente, si tratterà sempre di tentativo di truffa criminosa perpetrati al fine di carpire le credenziali dello stesso, al quale potrà essere imputata, come per legge, la piena responsabilità di qualunque conseguenza discendente e conseguente dalla comunicazione a terzi, anche se accidentale e involontaria, dei propri Dati/credenziali.

e) Evitare di includere nei messaggi allegati di dimensioni spropositate che hanno l'effetto di rallentare l'intero sistema e che spesso rischiano di essere rifiutati dal ricevente che a sua volta può essere vincolato a regole sulla dimensione massima ricevibile (il limite in Azienda è di circa 20MB, ma le caselle private -specialmente se gratuite- in genere hanno limiti inferiori): salvo eccezioni, un limite massimo che non dovrebbe essere mai superato è di ca. 10MB.

f) Accertarsi che il ricevente sia in grado di utilizzare i formati che utilizziamo negli allegati, attenendosi comunque il più possibile agli *standard*.

g) Scrivere messaggi sintetici che esplicitino subito il problema e che siano identificati da un oggetto chiaro.

h) Firmare sempre in modo esteso i propri messaggi con l'indicazione dei Dati necessari per l'identificazione e la reperibilità: questo processo può essere automatizzato impostando opportune opzioni nel programma di posta elettronica.

i) Inviare messaggi a una pluralità di destinatari solo se strettamente necessario: tali invii, infatti, appesantiscono molto il *server* di posta e la funzionalità complessiva del sistema; sono da evitare in particolare i messaggi frivoli o inutili, specialmente se inviati a molti destinatari.

j) È vietato l'utilizzo di tecniche di "*mail spamming*[21]": l'invio massivo di comunicazioni a liste di distribuzione Aziendali, *extra* Aziendali o di azioni equivalenti può essere effettuato esclusivamente da chi è autorizzato tramite l'Amministratore di Sistema.

[18] da intendersi come una valutazione se il contenuto della mail possa costituire un valore per l'attività istituzionale
[19] Termine di origine goliardica che definisce un insieme di messaggi inviati senza il loro permesso a una molteplicità di destinatari, comportamento considerato inaccettabile e ai limiti del fraudolento, anche perché l'elenco dei destinatari è spesso ricavato con metodi che possono collocarsi ai limiti della legalità. Lo scopo è in genere pubblicitario, ma spesso il messaggio spam può essere veicolo di informazioni denigratorie o offensive, a carattere politico, sessista o etnico. Inoltre, il proliferare dello spam ha un effetto deleterio soprattutto a causa dei costi, diretti o indiretti, del traffico generato dall'invio indiscriminato.
[20] Attività illegale che consiste in un tipo di truffa mediante la quale il criminale cerca di ingannare la vittima, per es. imitando un'entità, un aspetto e un contenuto affidabili o abituali per la vittima (esempio: Poste Italiane, la propria Banca *ecc*.), convincendola così a fornire informazioni personali, dati finanziari o codici di accesso segreti di cui poi farà un utilizzo improprio o illegale.
[21] Lo spam è l'invio di messaggi di posta elettronica pubblicitari e/o truffaldini che l'Utente non ha richiesto.

k) Sono da evitare, anche se considerati socialmente simpatici e graditi, i messaggi augurali in occasione di festività o eventi particolari: l'invio multiplo di tali messaggi, infatti, soprattutto se associato a un utilizzo spropositato della funzione "rispondi a tutti" dà luogo a catene d'invii che rapidamente possono paralizzare l'intero sistema di posta e in ogni caso appesantire inutilmente l'attività ordinaria.

l) Oltre che per la ragione esposta al punto precedente, per problemi di riservatezza, si deve sempre utilizzare con molta cautela l'opzione "rispondi a tutti": non sempre, infatti, è opportuno che tutti i destinatari del messaggio cui si risponde abbiano visibilità della risposta. Spesso si commettono involontari illeciti inviando Dati e informazioni riservate a destinatari inaspettati e inappropriati, solo perché questi sono presenti in un lungo elenco di destinatari precedenti al quale non si fa caso. Inoltre spesso gran parte dei destinatari di una "risposta a tutti" non è realmente interessato e coinvolto nel contenuto della risposta che, al contrario, si rivela spesso inutile e fastidiosa.

m) Utilizzare con altrettanta cautela l'opzione di "inoltro", in modo particolare evitare la trappola della diffusione della versione elettronica delle cosiddette "catene di Sant'Antonio": nel 99% dei casi i messaggi che invitano alla diffusione sono delle truffe (i casi della bambina con la leucemia da aiutare e simili sono i più diffusi...) e anche per rispetto del ricevente è sempre meglio verificare l'attendibilità dei messaggi prima di inoltrarli (è facile farlo con semplici ricerche su *Internet*).

n) L'inoltro automatico e il rinvio delle *e-mail* a una diversa casella di posta elettronica, specie se privata, non sono in genere consentiti salvo specifica autorizzazione per necessità particolari, in seguito a richiesta formale motivata; l'Utente può comunque attivare autonomamente l'inoltro dalla *webmail*, sotto la propria responsabilità.

o) In caso di assenza prolungata, per non ingenerare inutili aspettative nel mittente, ma anche per semplice cortesia, impostare il sistema in modo che sia restituito al mittente un messaggio appropriato nel quale lo si avvisi dell'impossibilità di una risposta immediata.

12.8. Considerazioni sull'attendibilità dell'identità del mittente di posta elettronica

Si deve sempre tener presente che, date le caratteristiche intrinseche dei sistemi di posta elettronica, è tecnicamente impossibile garantire l'identità e la veridicità del mittente. Esso, infatti, può essere falsificato agevolmente grazie a accorgimenti tecnici di modesta complessità che non richiedono particolari conoscenze informatiche. Lo stesso vale per loghi e altri elementi distintivi presenti all'interno dei messaggi che possono essere copiati e falsificati senza difficoltà.

12.9. Sistemi di sicurezza

Come tutti i sistemi di gestione della posta elettronica il sistema di ASP è aperto alla ricezione di messaggi provenienti dall'esterno e quindi è anche esposto agli abusi che ne possono derivare. I più frequenti si possono classificare a grandi linee in:

- *Virus* informatici e programmi dannosi in generale, che si propagano tramite posta elettronica e danneggiano o compromettono per varie vie i sistemi informatici.
- Posta pubblicitaria o indesiderata (*spam*).
- Tentativi di truffa e raggiri di varia natura tra cui: finte proposte di transazioni economiche, messaggi contraffatti apparentemente provenienti da banche o altre istituzioni con indirizzi di siti che imitano abilmente gli originali, proposte di lavoro ingannevoli, finte proteste e diffide, invio di false fatture o bollette, pubblicità di siti ingannevoli (tipicamente orientate al furto dei numeri di carta di credito, conto corrente, carte prepagate) *ecc.*

Questi abusi provocano in genere perdita di tempo e spreco di risorse, ma nei casi più gravi possono provocare danni anche rilevanti all'individuo e all'Azienda. In linea teorica il fenomeno si verifica anche con i *fax* e la posta tradizionale, tuttavia i bassissimi costi associati all'invio di messaggi di posta elettronica e la diffusione mondiale dei potenziali truffatori hanno amplificato a dismisura le dimensioni del problema.

A salvaguardia dell'integrità del sistema e a tutela degli utilizzatori sono attivi i seguenti sistemi di sicurezza:

- filtri *antivirus* per la protezione della posta elettronica;
- blocco alla ricezione/trasmissione *e-mail* di tutti gli allegati di tipo eseguibile o di altri tipi potenzialmente dannosi;
- filtri *anti-spam*;
- sistemi di *content inspection* che bloccano i messaggi analizzandone il contenuto;
- sistemi di blocco da *black list* che bloccano i messaggi in quanto provenienti da mittenti noti come non attendibili o pericolosi;
- blocco di auto-esecuzione da supporti di memoria esterni;
- blocchi della navigazione verso siti malevoli o con contenuti potenzialmente pericolosi;
- filtri *anti-spam* e di navigazione dinamici e aggiornati costantemente.

Come già ribadito, non essendo tali sistemi in grado di bloccare ogni tipo di attacco, è richiesta la massima attenzione da parte degli utilizzatori dei sistemi aziendali:

→ in caso di dubbi circa la presenza di *virus* in allegati a messaggi di posta elettronica, o in *link* presenti nel messaggio, il destinatario è invitato a non aprirli, o a non cliccare sui *link*: se necessario, contattare sempre il S.I.;

→ nel caso il *software antivirus* rilevi e segnali la presenza di un virus, l'Utente dovrà sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al S.I.

In ogni caso fare sempre riferimento alla procedura aziendale di *Data Breach*[22].

12.10. Gestione della casella di posta elettronica in caso di assenza dell'Utilizzatore/Utente

In caso di assenza programmata (esempio: ferie, attività di lavoro fuori sede, *ecc.*):

→ si raccomanda all'Utente di attivare l'opzione d'invio automatico di un messaggio di risposta contenente l'indicazione di un altro indirizzo di posta elettronica aziendale cui fare riferimento indicando eventualmente altre utili modalità di contatto della struttura.

In caso di assenza non programmata e prolungata (esempio: malattia, *ecc.*):

→ la procedura di risposta automatica – deve essere attivata dall'Utente nel più breve tempo possibile.

In caso di assenza improvvisa o prolungata e di impedimento dell'Utente di attivare la funzionalità di cui sopra e/o in caso di improrogabili necessità legate all'attività lavorativa:

→ l'accesso alla casella di posta, nei limiti e nel rispetto della normativa e delle Linee Guida del Garante, potrà essere effettuato dal S.I. ai soli fini dell'attivazione di messaggio d'avviso ai potenziali Mittenti per informarli della necessità di indirizzare i messaggi ad altro soggetto/indirizzo ASP .

12.11. Gestione della casella di posta elettronica in caso di cessazione del rapporto di lavoro o revoca assegnazione.

La cessazione del rapporto di lavoro, o delle condizioni che hanno portato al rilascio della casella *e-mail*, comporta la sua disattivazione immediata o comunque nel rispetto delle tempistiche previste dalla normativa vigente al tempo della cessazione e in accordo con le indicazioni dell'Autorità Garante della *Privacy*: pertanto i relativi messaggi ivi contenuti e di cui alla prestazione lavorativa del titolare dell'*account* saranno conseguentemente rimossi e cancellati dal *server mail*.

L'Azienda, infatti, contestualmente alla cessazione del rapporto di lavoro o delle condizioni che hanno comportato l'assegnazione di una casella di posta dell'Utilizzatore, è tenuta, nel rispetto di quanto definito dalla normativa vigente in materia di Trattamento dei Dati personali, a rimuovere *l'account* dell'interessato, previa disattivazione dello stesso senza possibilità di accesso, scarico e conservazione delle relative *e-mail* .

Invero, in adesione alle succitate prescrizioni del Garante della *Privacy*, il mantenimento della documentazione come prevista normativamente e/o come opportuna ai fini dell'operatività e

[22]Allegato C) alla Delibera di approvazione del presente Documento

organizzazione aziendale, non può essere effettuata attraverso la prolungata conservazione su *server* di posta elettronica bensì deve realizzarsi con modalità diverse, secondo le appropriate misure organizzative e tecnologiche adottate in Azienda e di cui anche al presente Regolamento.

Non è ammesso all'(ex)intestatario della casella di posta elettronica prelevare massivamente il contenuto della casella di posta e degli altri strumenti forniti, né conservarlo dopo la cessazione del rapporto di lavoro o delle condizioni che hanno portato al rilascio di tali funzionalità stante che i Dati contenuti, per effetto di questo stesso Regolamento, sono da intendersi esclusivamente inerenti all'attività lavorativa o di collaborazione e sono considerati riservati e di proprietà dell'Azienda e non dell'intestatario della casella e degli strumenti gestionali: pertanto un eventuale (anche tentato) accesso alla casella di posta effettuato dell'*ex* intestatario successivamente alla cessazione del rapporto di lavoro (a qualunque titolo intervenuta) o alla revoca dell'assegnazione dell'*accoun*t di posta risulterebbe illecito e come tale punibile ai sensi di legge (es: art. 615 ter C.P.).

Fermi restanti, quindi, gli obblighi di conservazione previsti *ex lege* e l'attività di conservazione documentale, svolta con le predette modalità alternative (cui, in costanza di rapporto di lavoro il dipendente deve riferirsi) resta inteso che l'*ex* dipendente/assegnatario potrà sempre richiedere l'accesso ai documenti aziendali dallo stesso ritenuti opportuni e necessari alla propria difesa (in caso di vertenza) e/o la loro produzione ed esibizione davanti all'Autorità competente secondo le procedure di legge previste (es: reclamo al Garante della *Privacy*, richiesta di esibizione documentale in giudizio *ecc*.).

A disattivazione della casella di posta effettuata, in caso di invio alla stessa di messaggio, il relativo mittente potrà ricevere giusta comunicazione di avviso ("*account disattivato*") corredato da eventuale indicazione di nuovo nominativo e indirizzo cui rivolgersi.

Eventuali eccezioni di quanto previsto nella presente clausola 12.11 dovranno essere autorizzate dalla Direzione Aziendale:

- qualora compatibili con la normativa vigente e le prescrizioni dell'Autorità Garante della *Privacy*;
- con adeguata motivazione che espliciti le circostanze di fatto e/o di diritto che giustifichino dette eccezioni;
- in risposta a casi di urgenza e necessità contingenti non previsti e non prevedibili;
- per un periodo di tempo corrispondente alla transitorietà della predetta urgenza/necessità imprevista e dovranno essere tempestivamente comunicate all'Interessato.

12.12. Accesso alla casella di posta elettronica per ragioni di sicurezza o manutenzione

Quando motivi di sicurezza o di manutenzione lo richiedano, il S.I., previo avviso agli Utenti interessati e anche in assenza di questi se impossibilitato a raggiungerli, può accedere alla configurazione delle caselle di posta elettronica per le sole finalità di sicurezza e manutenzione e per esclusive finalità tecniche.

L'accesso alla configurazione di posta non comporta la visualizzazione dei messaggi della casella, salvo il caso eccezionale in cui il problema di sicurezza o di manutenzione non possa essere risolto. In quest'ultimo caso, l'avviso all'interessato viene rinnovato prima dell'accesso ai messaggi contenuti nella casella, fermo restando che l'accesso dell'amministratore di sistema avverrà esclusivamente per motivi di sicurezza o manutenzione come sopra precisato.

L'attività effettivamente eseguita sulle configurazioni (o sui messaggi di posta, nel caso eccezionale di cui al periodo che precede), viene sempre comunicata all'Utente interessato al termine dell'intervento.

13. Utilizzo della rete *Internet*

13.1. Definizioni e strumenti

Accesso a un sito *Internet*

A ogni punto della rete *Internet* visibile pubblicamente è associato un numero identificativo (denominato indirizzo IP pubblico) che può anche essere utilizzato direttamente per l'accesso.

Tuttavia, per semplificare molto la gestione, l'indirizzo IP è trasformato dal sistema *Internet* in un testo comprensibile che identifica in modo esplicativo il punto della rete richiesto - indirizzo del sito *Internet*: per esempio il sito *Internet* dell'Azienda ha l'indirizzo: www.aspbologna.it. - Digitando questo testo nel programma di accesso si raggiunge direttamente il sito desiderato.

L'intero indirizzo comprensivo delle indicazioni relative al protocollo e alla pagina desiderata è denominato *URL* (*Universal Resource Locator*: per esempio la pagina di presentazione dell'Azienda ha *URL*: https://www.aspbologna.it/). Infine anche l'*URL*, che può essere costituito da un testo molto lungo o complicato, può essere a sua volta mascherato da un elemento grafico o testuale di una pagina (così detto *link*) cliccando il quale si attiva la connessione corretta.

In genere il punto cui si accede costituisce un "sito *Internet*" quando è organizzato in un insieme di contenuti (pagine), collegati tra loro secondo una precisa gerarchia (ipertesto), mediante l'utilizzo di appositi strumenti informatici. Tali contenuti si possono consultare agevolmente utilizzando esclusivamente il mouse o altri strumenti messi a disposizione per garantire l'accessibilità. Il termine "navigazione" (in *Internet*) nasce appunto da questa modalità di consultazione che consente di spostarsi da un argomento all'altro e da un punto all'altro della rete con grande semplicità e velocità.

Connessione a *Intranet*

L'Intranet è il sito interno aziendale che è costituito dal complesso sistema d'informazioni e di servizi di utilità generale accessibili solo dalla rete interna. Tale sito può essere reso disponibile anche all'esterno della rete aziendale, in questo caso si parla di *Extranet*.

Tutti i dipendenti e collaboratori aziendali hanno accesso alla rete *Intranet* e sono invitati a prendere sempre visione dei suoi contenuti informativi.

13.2. Abilitazione alla connessione *Internet*

La navigazione in *Internet* viene abilitata in modo selettivo per tutte le postazioni e gli Utenti che facciano parte di un dominio riconosciuto.

Salvo diversa indicazione da parte del Soggetto *Sub*-Delegato Attuatore del Trattamento (o del Soggetto Delegato Attuatore, secondo il caso) ogni dipendente, mediante le proprie credenziali di dominio (già inserite all'atto di accesso al *p.c.*), può navigare in *Internet* da qualsiasi stazione di lavoro con queste abilitata.

Per motivi di sicurezza stazioni di lavoro particolarmente critiche per il tipo di attività effettuato o per il tipo di Dati gestiti non vengono abilitate alla navigazione in Internet: Soggetto *Sub*-Delegato Attuatore del Trattamento (o del Soggetto Delegato Attuatore, secondo il caso).

Per accedere al servizio l'Utente deve fornire i propri Dati identificativi, poiché non è consentito alcun tipo di accesso anonimo. L'Utente, inoltre, deve attenersi strettamente al presente Documento e al regolamento per l'utilizzo dei sistemi informatici. In genere l'abilitazione è fornita senza altre particolari formalità, a meno che non ci sia una diversa indicazione da parte del Soggetto *Sub*-Delegato Attuatore del Trattamento di riferimento.

13.3. Utilizzo delle connessioni a *Internet*

L'abilitazione tramite dotazioni aziendali alla connessione e navigazione in *Internet* costituisce uno strumento/facoltà Aziendale utilizzabile esclusivamente per fini istituzionali quali:

- ☛ lo svolgimento dell'attività lavorativa e contestuale adempimento delle proprie mansioni, compiti e incarichi assegnati
- ☛ per ulteriori fini istituzionali di cui possa giovare l'Utente quali:
  - ✓ l'approfondimento delle conoscenze
  - ✓ la documentazione
  - ✓ l'accrescimento della professionalità

Conseguentemente, è assolutamente vietata la connessione e la navigazione in *Internet* per motivi diversi da quelli strettamente legati all'attività lavorativa, *sub* 13.3. punti 1 e 2.

Pertanto, a titolo meramente esemplificativo e senza pretesa di esaustività, è sempre tassativamente vietata la connessione e la navigazione a:

a. *siti a carattere ludico e di intrattenimento*: la definizione va intesa in senso lato e include tutti i siti inerenti anche in senso generico all'intrattenimento e/o all'organizzazione del tempo libero (giochi *on-line*, case discografiche, agenzie di viaggi, proposte di vacanze, strutture di accoglienza alberghiera, agenzie e compagnie aeree, sistemi di trasporto, ristoranti *ecc.*). Rientrano in questa esclusione anche i siti commerciali cui si acceda per uso personale (per esempio: concessionari o case automobilistiche, centri commerciali, fabbricanti e distributori di prodotti di consumo o servizi, *ecc*.), nonché le testate giornalistiche *on-line*, nonché i siti di associazioni e i siti a carattere religioso o politico;

b. *siti a carattere erotico e pornografico*: la definizione va intesa in senso lato e include tutti i siti inerenti anche in senso generico alla trattazione o raffigurazione di soggetti erotici o di carattere osceno. Si ricorda che l'accesso a taluni siti (per esempio a contenuto pedo-pornografico) costituisce un reato;

c. *siti che consentano transazioni commerciali e pagamenti on-line*: non è consentita l'esecuzione di transazioni commerciali che presuppongano o meno un pagamento *on-line* per l'acquisto di prodotti e servizi;

d. *siti interattivi*: In questa categoria rientrano vari tipi di servizi quali le conversazioni scritte (esempio: *chat*, *messenger, ecc.*) e telefoniche *online* (esempio: *skype*, *VoIP, ecc.*), che restano vietate a meno che non siano utilizzate per uso istituzionale (esempio: partecipazione a *meeting on-lin*e, attività di assistenza, corsi di formazione*, ecc.*); la compilazione di modulistica (*form*) *on-line*; la partecipazione a luoghi d'incontro su temi specifici (forum) o la partecipazione a *mailing list* non inerenti all'attività aziendale;

e. *caselle di posta personale;*

f. *area web personale su sociali media;*

g. *darknet;*

nonché:

h. l'*upload* e il *download* di:

- ✓ *software* anche gratuiti (freeware) e shareware, nonché documenti provenienti da siti *web* o *http*, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (in caso di dubbio contattare il S.I.);
- ✓ *file* musicali, video, immagini, programmi, aggiornamenti sia in forma gratuita sia in seguito a transazione commerciale;

nonché:

i. l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, fatti salvi i casi direttamente autorizzati dal Soggetto *Sub*-Delegato Attuatore del Trattamento e comunque nel rispetto delle normali procedure di acquisto;

nonché:

j. la partecipazione a *forum* non professionali, l'iscrizione con account Aziendale e la partecipazione personale a *social network*, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in *guest books* anche utilizzando pseudonimi (o *nickname*) se non espressamente autorizzati dal Responsabile d'ufficio*;*

Fa eccezione al divieto generale di cui sopra, la possibilità di:

- ☛ *Upload* e *download* di *file* utilizzati per la propria funzione aziendale con la sola limitazione a copie di documenti (in genere in formato testo, *word* o *pdf*) o d'immagini da inserire nei propri documenti;
- ☛ *Download* di *software* e loro aggiornamenti nel caso sia ritenuto necessario per l'attività lavorativa e previa diversa autorizzazione scritta del S.I. su richiesta motivata;
- ☛ *Upload* su *Internet* dei *file* aziendali, eccetto i casi previsti dall'attività istituzionale.

Inoltre, l'utilizzo di *Internet* per svolgere attività che non rientrino tra i compiti istituzionali può essere consentito, nei limiti del carattere di eccezionalità e saltuarietà, per esigenze personali ed

esclusivamente per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro e nei tempi strettamente necessari allo svolgimento delle transazioni (esempio: per effettuare adempimenti *on line* nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi *ecc.*).

13.4. Regole di buon comportamento per l'utilizzo di *Internet*

Di seguito alcune indicazioni e regole di buon senso cui l'Utente deve attenersi nell'utilizzo dei sistemi di comunicazione.

a) Limitare la connessione al solo tempo necessario alle operazioni richieste: anche la connessione inattiva, infatti, consuma le risorse del sistema rendendolo meno disponibile agli altri utilizzatori.

b) Controllare accuratamente la correttezza degli indirizzi a cui ci si connette e la qualità delle informazioni in essi contenute: va sempre ricordato, infatti, che *Internet* è un mondo assolutamente libero nel quale chiunque può inserire informazioni anche se non è autorizzato e/o qualificato per farlo; inoltre chiunque, con estrema facilità, può costruire ad arte un sito millantando conoscenze, titoli o qualifiche false o inesistenti.

c) Valutare con razionalità il contenuto delle pagine visitate evitando di cadere in truffe e/o altri abusi: in particolare va evitato l'inserimento dei propri Dati anagrafici o di altre informazioni personali in moduli di acquisizione *on-line*. A maggior ragione evitare l'inserimento di Dati altrui (in questo caso il comportamento da incauto si trasforma in vero e proprio illecito).

d) Nel caso si utilizzi *Internet* per comunicare/ricevere Dati personali e in particolare Dati sensibili (es. per compilazione di moduli *online*, *upload* o *download* di documenti personali, *ecc*.), l'Utente è tenuto a verificare che vengano utilizzati canali di comunicazione sicuri, o, comunque, che adottino idonee tecniche di cifratura (HTTPS/SSL/VPN, crittografia) o altri sistemi di sicurezza (esempio: credenziali dedicate, *One Time Password, ecc.*): nel caso non sia in grado di verificare la sicurezza del canale di trasmissione, l'Utilizzatore può fare riferimento al S.I.

e) Utilizzare in modo preciso e consapevole i motori di ricerca per evitare inutili perdite di tempo o risultati inattesi.

f) Ricordare che la disponibilità su *Internet* di documenti, immagini e *file* di qualsiasi genere non garantisce che questi siano liberamente prelevabili o utilizzabili: non vale la buona fede ma, al contrario, vale sempre:

- ✓ la preliminare verifica della loro autenticità, attribuibilità e attendibilità;
- ✓ la restrittiva normativa sul diritto d'autore che configura la copia e/o l'utilizzo illegale come un reato penale (anche qualora eventuali informazioni sul *copyright* non siano immediatamente evidenti); in modo particolare occorre accertarsi della sussistenza di eventuali diritti di *copyright* prima di inserire in propri documenti (per esempio in *word* o in presentazioni *powerpoint*) immagini, Dati, informazioni o altro prelevati in qualsiasi modo da *Internet*.

g) Ancora in merito al tema del diritto d'autore, va precisato che le normative dei diversi Stati (soprattutto extraeuropei) sono differenti tra loro, anche di molto, pertanto ciò che è reso disponibile in quanto lecito in un determinato stato potrebbe non esserlo nel nostro Paese (basti pensare alla facilità con cui è possibile reperire in rete brani musicali che sono con tutta evidenza soggetti a vincoli di *copyright*): si rammenta in proposito che il solo possesso di tali *file* può dar luogo alla contestazione di un reato penale, se dimostrabile il fine di lucro[23].

13.5. Responsabilità in merito all'utilizzo di *Internet*

A sensi e per gli effetti tutti di legge, l'Utente è direttamente e totalmente responsabile dell'uso del servizio di accesso a *Internet*, dei contenuti che vi ricerca, dei siti che contatta e consulta, delle informazioni che recupera o vi immette e delle modalità con cui opera. È responsabile inoltre delle conseguenze di qualsiasi natura che derivino dal loro utilizzo.

[23] nota bene: anche il semplice mancato pagamento dei diritti è stato considerato tale in alcune sentenze

13.6. Responsabilità in merito all'accesso a *Internet*

L'Utente è Titolare e responsabile della corretta conservazione della propria credenziale di autenticazione (*account* e *password*), che deve essere nota a lui soltanto: ogni accesso avvenuto con tale credenziale (che deriva indirettamente dall'accesso al sistema all'accensione del *P.C.*), infatti, sarà sempre imputato a lui come assegnatario. È vietato, pertanto, lasciare incustodita senza opportuno blocca schermo la postazione di lavoro assegnata: una persona diversa dall'assegnatario che abbia accesso anche temporaneo al *P.C.*, infatti, potrebbe accedere a *Internet* con le credenziali dello stesso senza che questi ne abbia visibilità.

13.7. Revoca delle credenziali o dei diritti di accesso a *Internet*

L'accesso a *Internet* può essere revocato o non concesso nei seguenti casi:

a) qualora se vengano meno le condizioni per il rilascio dell'autorizzazione (per es. per cessazione della condizione di dipendente o collaboratore autorizzato);

b) in caso di accertamento di un uso non corretto del servizio anche in violazione del presente Regolamento;

c) in caso di diffusione o comunicazione imputabili direttamente all'Utente d'informazioni riservate (inclusa la propria credenziale di accesso) anche in violazione della normativa *privacy*;

d) in caso di richiesta formale e motivata da parte del Responsabile del Servizio di appartenenza.

13.8. Sistemi di sicurezza e categorie di siti bloccate da sistemi automatici

Per garantire la sicurezza della postazione e dell'Utilizzatore, oltre al blocco selettivo dei siti ritenuto non d'interesse istituzionale, l'Azienda si è dotata dei seguenti sistemi di sicurezza:

a) filtri *antivirus* per la protezione della navigazione web;

b) blocco allo scaricamento, volontario o involontario, di file compressi non sicuri e file eseguibili o di altra natura ritenuta pericolosa, dannosa o non pertinente, durante la navigazione Internet;

c) filtri alla navigazione sulla base di sistemi di classificazione dei contenuti dei siti.

Fermi restando i divieti precedentemente elencati anche se i siti non sono bloccati dal sistema di controllo, questo inibisce in modo preventivo l'accesso a molti siti inserendoli nella così detta "*black list*", anche se non è in grado di mappare tutti i siti indesiderati.

A titolo di esempio alcune delle categorie bloccate sono:

→ *Hacking: s*iti *web* che promuovono attività illecite per la modifica non autorizzata di *software* o l'accesso ai programmi, *computer*, attrezzature e siti *web*.

→ *Malware: s*iti che contengono software dannoso o distruttivo specificamente progettato per danneggiare, interferire, attaccare o manipolare sistemi informatici, senza il consenso dell'Utente, come per esempio virus, cavalli di troia o *worm*.

→ *Spyware: s*iti che ospitano software che sarà scaricato all'insaputa dell'Utente del *P.C.*, per raccogliere informazioni personali e monitorare le attività del sistema, compresi *spyware, adware* ecc.

→ *Phishing: s*iti che falsificano o clonano pagine *web* di banche, finanziarie, carte di credito *ecc*. al fine di carpire la fiducia dell'Utente e rubare le *password* di accesso o altre informazioni personali.

→ *Proxy Avoidance:* siti *web* che forniscono informazioni o strumenti su come aggirare i controlli di accesso a Internet e navigare nel *Web* anonimo.

→ *Pornografy: s*iti con contenuti per adulti (18 anni e oltre) che presentano o mostrano atti sessuali espliciti.

→ *Adult Material:* siti con contenuti per adulti (18 anni e oltre) che offrono o promuovono la sessualità, strip club, *sex-shop ecc*.

→ *Game: s*iti di giochi online per computer e relativi collegamenti, concorsi, promozioni *ecc.*

→ *Gambling: s*iti che promuovono e organizzano gioco d'azzardo, scommesse, lotterie, case da gioco *ecc.*

→ *Personal Relationship:* siti *web* per la gestione di gruppi e amicizia. Include siti di annunci personali, servizi di incontri, club non sessuali, *ecc*.

13.9. Pubblicazione di contenuti e realizzazione di siti personali

L'Utente non è autorizzato in alcun caso a produrre e a pubblicare siti *web* personali utilizzando risorse aziendali né a pubblicare autonomamente siti riferiti alla struttura di appartenenza.

Ogni eventuale necessità di realizzare siti *web* personali o di struttura utilizzando risorse aziendali dovrà essere espressamente autorizzata.

È fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza autorizzazione della Direzione Aziendale.

È fatto divieto agli utenti di inserire nei siti personali collegamenti (*link*) al sito Aziendale senza autorizzazione della Direzione Aziendale.

Si applicano in ogni caso, ove applicabili, le norme dei Codici deontologici professionali.

È fatto assoluto divieto di realizzare funzioni di *Hosting* utilizzando risorse aziendali.

13.10. Connessione a *provider* diversi da quello aziendale

È vietato l'utilizzo di accessi *Internet* mediante *Internet Provider* diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti *Provider*, anche con abbonamenti privati.

Infatti tali connessioni rappresentano un potenziale rischio per la sicurezza dell'intero sistema informativo aziendale di cui l'Utente è pertanto responsabile.

13.11. Utilizzo di *server* esterni per *backup*, gestione, e condivisione dei documenti aziendali

Salvo casi particolari che devono essere espressamente autorizzati, è vietato caricare documenti aziendali riservati e contenenti Dati di natura sensibile su sistemi di memorizzazione esterni (esempio: *cloud* quali *Dropbox*, *SkyDrive*, *icloud, ecc*.) che non siano appartenenti al *Cloud* eventualmente previsto in ASP e a tale fine autorizzato.

Ciò in quanto tali sistemi possono essere soggetti ad attacchi informatici e i Dati possono essere sottratti o manipolati illegalmente. Inoltre tali sistemi potrebbero essere ospitati in Paesi non soggetti a regolamentazioni sulla *privacy* analoghe a quella europea.

Non saranno pertanto effettuate abilitazioni specifiche che permettano la connessione a tali sistemi, salvo casi particolarissimi da valutare e autorizzare singolarmente (per esempio accessi temporanei per prelevare Dati da gruppi di lavoro già esistenti).

Gli Utenti aziendali dotati di *Office* nella versione *online* possono accedere a *OneDrive*[24] mediante credenziali aziendali; infatti in tal caso si ha la garanzia che i Dati siano conservati nell'Unione Europea, secondo la relativa normativa di protezione dei Dati, tuttavia permane il divieto di collocare su tale *cloud* Dati riservati o di natura sensibile.

Gli Utenti aziendali possono utilizzare i sistemi di collaborazione messi a disposizione da Google Workspace nell'ambito degli account aziendali assegnati.

13.12. Assistenza da remoto (VPN e altre tipologie)

Sono ammessi collegamenti remoti dall'esterno per l'accesso alle risorse aziendali, sia per manutenzione di attrezzature da parte di ditte esterne, sia per lo svolgimento di specifiche attività da una sede esterna, ma devono essere autorizzati dal S.I.

13.13. Utilizzo delle cartelle condivise

Per la conservazione di Dati e documenti di lavoro a carattere continuativo e funzionale alla propria attività, l'Azienda mette a disposizione spazi di archiviazione di dimensione variabile denominati

[24] Si tratta del servizio fornito da Microsoft con il pacchetto Office 365 online

cartelle condivise. Questi spazi consentono pertanto di condividere le informazioni all'interno del proprio servizio o tra servizi differenti.

Come già detto per lo spazio disco della propria stazione di lavoro, non è consentito conservare nelle cartelle condivise Dati e documenti contenenti Dati sensibili.

L'utilizzo delle cartelle condivise deve essere razionalizzato e appropriato alle reali attività gestite, in quanto esso costituisce un costo per ASP, sia in termini delle risorse infrastrutturali sottostanti, sia in termini di costi indiretti di mantenimento dell'infrastruttura stessa: si veda altresì quanto previsto *sub* 9.8 .

14. Utilizzo dello *smartphone* aziendale

Al fine di assicurare il servizio di pronta reperibilità e lo svolgimento dell'attività istituzionale, ASP fornisce *smartphone* aziendali ai propri dipendenti, previa valutazione da parte del relativo Responsabile di Servizio.

Di norma l'abilitazione del telefono aziendale è limitata alle sole chiamate, tuttavia è possibile abilitare i telefoni alla trasmissione Dati, sempre previa richiesta del Responsabile di afferenza, il quale assume l'onere di vigilanza sul corretto utilizzo del dispositivo.

Tra gli utilizzi impropri del telefono cellulare aziendale rientra la comunicazione di Dati di natura sensibile (referti, radiogrammi o qualunque altra informazione relativa alle attività cliniche) attraverso *network* digitali come ad esempio *WhatsApp* salvo autorizzazione del Responsabile di afferenza.

Tale tipo di comunicazione è dunque vietata.

Non è consentito all'autorizzato caricare o inserire all'interno dello *smartphone* o della *SIM* qualsiasi Dato Personale non attinente all'attività lavorativa svolta.

I Dati salvati sullo *smartphone* (rubrica, agenda) sono sotto la responsabilità del singolo Utente, che deve occuparsi di provvedere ai necessari backup o salvataggi.

In caso d'interruzione del rapporto di lavoro tutti i Dati aziendali presenti nello *smartphone* (es. rubrica telefonica) devono essere restituiti unitamente all'apparecchio.

Al fine di evitare e/o ridurre al minimo la possibile circolazione di Dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti/solo i Dati non attinenti all'attività lavorativa eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione.

Non è consentito manomettere i componenti del dispositivo.

Non è consentito effettuare operazioni di programmazione non previste dal manuale d'uso.

È vietato lasciare lo *smartphone* aziendale in automobile, anche se posizionato nel baule e anche se l'auto è chiusa a chiave.

L'Azienda si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla *SIM* in questione per il periodo interessato.

15. Modalità di prestazione dei servizi

Il S.I. s'impegna a fornire continuità ai servizi erogati, riservandosi la possibilità di interromperli esclusivamente per le manutenzioni ordinarie e cercando di arrecare il minor disagio possibile agli utilizzatori: salvo impedimenti, le interruzioni saranno comunicate agli utenti.

Per poter fornire assistenza e supporto tempestivi nel caso di guasti e malfunzionamenti, su ciascun *P.C.* (fisso o portatile) è installata un'applicazione che consente ai tecnici del S.I. di collegarsi da remoto, senza bisogno di intervenire sul luogo.

Pertanto la manutenzione alle stazioni di lavoro viene generalmente effettuata, in prima battuta, mediante tali sistemi *software* di manutenzione remota: solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento *in loco*.

I suddetti sistemi di controllo remoto sono configurati affinché gli operatori che intervengono per la manutenzione possano farlo esclusivamente previo consenso dell'Utilizzatore della postazione (consenso che viene richiesto in tempo reale sullo schermo del *P.C.*); non sarà richiesta l'autorizzazione solo nei casi in cui si renda necessario effettuare installazioni e/o aggiornamenti *software* da remoto, che non prevedono la possibilità di accesso ai Dati presenti.

Inoltre l'Utente può verificare l'attività effettuata in remoto dal tecnico rimanendo presso la postazione.

Gli interventi possono essere eseguiti da personale identificato e autorizzato da ASP tramite contratti di fornitura di servizi.

16. Installazione di *Microsoft Office* sulle postazioni di lavoro

Per quanto riguarda i programmi di utilità e di automazione d'ufficio (elaborazione testi, fogli elettronici, presentazioni) lo *standard* aziendale prevede l'utilizzo di Google Workspace, pertanto non sarà più fornito il sistema *MS Office e Open Office*.

Sono previste eccezioni per esigenze specifiche che devono essere adeguatamente motivate e autorizzate, quali:

⇒ procedure aziendali che richiedano necessariamente l'utilizzo di *MS Office - Open Office*;

⇒ necessità di compatibilità con vecchie procedure *Access*.

Si precisa che le licenze di *MS Office* installabili sui *P.C.* aziendali sono solo quelle acquistate da ASP (non sono ammesse né licenze personali né licenze universitarie).

17. Utilizzo dei sistemi di videoconferenza

L'Azienda consente l'utilizzo di sistemi di videoconferenza (di cui all'utilizzo di piattaforme digitali o *social media*) per le videocomunicazioni afferenti direttamente o indirettamente il servizio tra dipendenti, collaboratori e soggetti terzi invitati in riunioni o incontri in remoto organizzate da personale di ASP qualora detto utilizzo risponda a un'esigenza di carattere istituzionale.

L'utilizzo di sistemi di videoconferenza per il colloquio con i pazienti o per televisite di controllo è consentito esclusivamente mediante sistemi autorizzati esplicitamente da ASP.

18. Lavoro Agile (c.d. *Smartworking*)

Le prescrizioni del presente Regolamento, come nel caso applicabili, valide e vincolanti altresì nei casi di *smartworking* aziendale[25], che alla data odierna prevede:

⇒ in via principale: l'impiego di *laptop* aziendali assegnati al Dipendente in regime di *smartworking*;

⇒ in via residuale: l'utilizzo da parte dello *smartworker* del *P.C.* personale (esterno ad ASP) quale strumento di accesso e collegamento da remoto (realizzato e supervisionato dal S.I.) al *P.C.* assegnato e presente presso i locali aziendali[26];

precisando che ASP ha dato seguito a investimenti finalizzati a reperire le dotazioni tecniche (acquisto di nuovi *laptop*), cui dotare l'interezza del Personale interessato dalla modalità di *smartworking*e e quindi proseguire nella dismissione della predetta procedura residuale, ancora in vigore per casi particolari.

[25] Per Lavoro Agile/*Smartworking* s'intende una modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le Parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, ma in ogni caso entro i confini del territorio nazionale: detta modalità viene riconosciuta al singolo Dipendente tramite un Accordo Individuale realizzato secondo le previsioni del D.M. 8 ottobre 2021 "*Modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni*" e delle *Linee guida in materia di lavoro agile nelle amministrazioni pubbliche* definite il 30 novembre 2021 (nelle more della sottoscrizione del nuovo CCNL.)
[26] Sul punto si rinvia anche a quanto *sub* 9.3.

19. Gli strumenti di controllo

19.1. L'utilizzo dei sistemi *software* applicativi aziendali

Per espresso vincolo normativo[27] l'accesso a qualsiasi sistema aziendale è soggetto a tracciamento, che avviene in modo diverso secondo il tipo di programma e il suo livello di aggiornamento[28]. Sono sempre tracciati i seguenti Dati:

- ✓ identificativo dell'Utente che ha avuto accesso;
- ✓ identificativo dell'Utente che ha operato sul sistema (inserimenti, cancellazioni, modifiche, visualizzazioni, *ecc.*);
- ✓ unità operativa di afferenza o di accesso;
- ✓ data e ora dell'operazione (di accesso, di modifica ecc.)
- ✓ data e ora.

Tali Dati sono raccolti in appositi *file* (*log*) che vengono conservati per un periodo di sei mesi salvo diverse indicazioni normative. L'accesso è limitato ai soli casi di necessità e riservato al solo personale tecnico autorizzato (amministratori di sistema).

L'Azienda è tenuta a verificare periodicamente la validità delle credenziali di accesso (che sono sospese in caso di perdita della qualità) e la liceità delle operazioni di Trattamento, agendo in conseguenza di eventuali trattamenti illeciti.

19.2. Gli accessi a *Internet*

Tutti gli accessi a *Internet* vengono registrati sul sistema di sicurezza Aziendale in appositi *file* di *log*, che tengono traccia dei seguenti Dati per ogni accesso:

- ✓ identificativo dell'Utente che ha navigato in internet;
- ✓ identificazione della stazione di lavoro;
- ✓ data e ora;
- ✓ riferimento al sito visitato (*URL*).

Tali *log* sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema, entrambi su base anonima. I *log* sono trattati per un massimo di una settimana esclusivamente per ragioni tecniche (esempio: per individuare un problema di blocco di navigazione), dopodiché sono trasformati in modo da fornire informazioni esclusivamente in forma aggregata, così da precludere l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni (per esempio: su richiesta dell'Autorità Giudiziaria) per accedere alle informazioni di dettaglio massimo.

19.3. L'utilizzo della posta elettronica

Il sistema di posta elettronica tiene traccia di tutte le *e-mail* inviate e ricevute, conservando nei *log*:

- ✓ data e ora;
- ✓ identificativo della stazione di lavoro che ha inviato il messaggio;
- ✓ indirizzo di posta del mittente;
- ✓ indirizzo del destinatario.

I *log* della posta e degli altri strumenti *cloud* sono conservati per un periodo minimo di sei mesi e per un periodo massimo di un anno.

19.4. La telefonia

ASP si riserva la facoltà, se del caso e nel rispetto della normativa tutta in materia, mediante configurazioni sugli apparati tecnologici, d'impedire l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri, quali i numeri a pagamento per servizi particolari. L'operatore

[27] in particolare le misure minime di sicurezza di cui alla Circolare AgID 2/2017
[28] Alcuni sistemi non del tutto adeguati alla normativo sono in via di dismissione.

che avesse la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione.

Per fini di controllo della spesa telefonica l'Azienda tiene traccia, attraverso i servizi del *provider* telefonico, delle telefonate effettuate, se queste costituiscono un onere economico per l'Azienda (mentre non sono, ad esempio, tracciate le telefonate in ingresso). In particolare viene registrato:

- ✓ il numero del chiamante;
- ✓ il numero chiamato;
- ✓ la data e ora d'inizio della telefonata e la data e ora di fine della stessa

Tutti i *log* sopra citati vengono conservati dall'Azienda per un anno solare nel formato originale per poter confrontare gli andamenti di costo con i Dati aggregati degli anni precedenti. I Dati disaggregati dal primo gennaio dell'anno al trentuno dicembre dell'anno potranno essere conservati fino alla fine di marzo dell'anno successivo per i controlli istituzionali, dopo di che dovranno essere aggregati in maniera tale che possano essere utilizzati per i confronti con i periodi successivi. I controlli verranno effettuati in maniera non nominativa e aggregata (ad esempio aggregando i Dati per edificio o per unità erogante): qualora i Dati evidenzino anomalie tali da giustificare controlli aggiuntivi, potranno essere ulteriormente approfonditi. Normalmente sarà necessario adottare una gradualità nei controlli che preveda prima il controllo del Dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui Dati disaggregati. Qualora l'integrità del sistema tecnologico dell'Azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al Dato disaggregato; qualora possibile, gli approfondimenti sui Dati che si rendessero necessari saranno condotti con verifiche a campione.

19.5. La registrazione delle conversazioni telefoniche

Non è ammesso l'utilizzo di sistemi di registrazione delle chiamate, in particolare se resi disponibili attraverso l'utilizzo di strumenti aziendali (*smartphone*, *tablet* ecc.), fatti salva la facoltà per ASP, per eventuali, singole eccezionali casistiche e necessità alle stesse correlate[29], di attivare appositi sistemi, di cui si darà prontamente notizia a tutti i soggetti interessati.

19.6. Facoltà di ASP

ASP, attraverso i propri responsabili di riferimento come coordinati dal S.I., ha facoltà di svolgere gli accertamenti necessari ad adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei *Dati*, in conformità alla modalità stabilite dall'Agenzia per l'Itali Digitale come aggiornate nel tempo.

In conformità al quadro normativo e alle disposizioni di legge in generale, ASP si riserva il diritto di effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature aziendali nel caso in cui accerti manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso, ovvero riscontri diffusioni indebite d'informazioni atte a pregiudicare la sicurezza del sistema stesso o il suo buon funzionamento e/o a garantire ad altri accessi o altri privilegi non dovuti, o ancora abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata.

In tali casi ASP può disabilitare le autorizzazioni all'accesso e all'uso delle attrezzature aziendali, segnalare al responsabile organizzativo situazioni e comportamenti anomali degli operatori, presentare denuncia all'Autorità Giudiziaria, in caso di reati perseguibili d'ufficio.

In caso di problemi inerenti alla sicurezza della infrastruttura tecnologica ASP si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni *software* e/o *hardware* ecc. Tutte le azioni messe in atto sono valutate in una logica di costo/beneficio e sono improntate a un criterio di minimizzazione del disservizio.

[29] Su richiesta stessa dei servizi interessati (a esempio per particolari e contingenti esigenze di tutela reciproca degli interessi dei soggetti parlanti); in tali casi ASP provvederà a pubblicare sul sito *web* la relativa informativa e configurare il risponditore in modo che avvisi della registrazione e della presenza dell'informativa sul sito, altresì specificamente normando l'accesso alle registrazioni.

ASP si riserva la facoltà di sospendere l'accesso ai servizi qualora, anche a seguito di segnalazioni del Soggetto *Sub*-Delegato Attuatore del Trattamento (o del Soggetto Delegato Attuatore, secondo il caso) sussistano nel tempo reiterate evidenze delle inadempienze da parte dell'operatore.

ASP si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni.

19.7. Limite dei controlli

In generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio di ASP; qualora le verifiche portino all'accertamento della violazione delle presenti regole e/o, più in generale, all'accertamento di utilizzi impropri, ASP si riserva di adottare le opportune misure disciplinari e amministrative, anche con accesso ai Dati di dettaglio necessari per il completamento dell'istruttoria nei limiti previsti dalla normativa applicabile in materia.

19.8. Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente regolamento, la disponibilità a un Utente dei servizi informatici aziendali cesserà totalmente nel caso non sussista più la condizione di dipendente o di collaboratore esterno; inoltre può cessare o essere limitata nei privilegi assegnati in caso di:

a) revoca dell'autorizzazione all'uso fornita dal Soggetto *Sub*-Delegato Attuatore (o dal Soggetto Delegato Attuatore, secondo il caso), per esempio per cambio di mansione, ruolo, servizio *ecc*.;

b) accertato uso non corretto o comunque estraneo alla sua attività lavorativa dei servizi informatici aziendali;

c) accertate manomissioni e/o interventi illeciti sul *hardware* e/o sul *software*;

d) accertate diffusione o comunicazione imputabili direttamente o indirettamente all'Utente, di *password*, procedure di connessione, indirizzo I.P. e altre informazioni tecniche riservate;

e) accesso illecito e intenzionale dell'Utente a *directory*, a siti e/o *file* e/o servizi da chiunque resi disponibili, in particolare se l'attività dell'Utente comporti danno, anche solo potenziale al sito contattato;

f) violazione delle regole essenziali stabilite dal presente Regolamento.

Si precisa che in caso di cessazione della condizione di dipendente o collaboratore a una certa data la casella di posta dell'Utente sarà immediatamente disattivata.

Si ricorda inoltre che, una volta cessata la condizione di dipendente o collaboratore è vietato asportare Dati aziendali prodotti nell'attività istituzionale. Non sarà Dato seguito, pertanto, alla richiesta di scarico massivo (per esempio: su supporto esterno) delle *e-mail* dell'Utente, né di altri file contenuti nei *file server* o nei *personal computer*.

19.9. Responsabilità dell'Utilizzatore delle risorse informatiche

L'Utente è direttamente e totalmente responsabile dell'uso che egli fa delle risorse informatiche assegnate, dei contenuti che tratta a mezzo del servizio di posta elettronica e di accesso a *Internet*, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

All'Utente è consentito di utilizzare le risorse informatiche solo per ragioni professionali connesse alla propria attività.

L'uso privato della posta elettronica, o non conforme alle prescrizioni contenute in questo regolamento, è tollerato se a carattere saltuario e trascurabile rispetto all'uso ordinario (ad esempio la ricezione/invio di *un'e-mail* personale sulla casella aziendale): esso, tuttavia, esonera ASP dall'incorrere nel reato di violazione di corrispondenza privata[30], nel caso specifico *sub specie* di cognizione della posta elettronica indirizzata al dipendente.

[30] Art. 616 c.p.

L'Utente prende atto che è vietato servirsi e/o dar modo ad altri di servirsi della rete Aziendale e dei servizi da essa messi a disposizione per utilizzi illeciti che violino e/o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private e/o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica e/o privata, per recare offesa e/o danno diretto e/o indiretto ad ASP e/o a terzi e ogni altra previsione di legge in materia.

19.10. Finalità e modalità del Trattamento

ASP s'impegna a trattare i Dati relativi all'utilizzo dei servizi informatici unicamente per motivi volti a garantire la sicurezza e il corretto funzionamento dei servizi informatici e per finalità direttamente pertinenti all'attività lavorativa del dipendente.

Le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate per finalità di sicurezza del sistema.

L'attività di registrazione avviene attraverso i file "*log*" di sistema a cura del S.I.

Per quanto riguarda l'utilizzo dei sistemi informativi aziendali, le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate al fine di garantire la tracciabilità del Trattamento dei singoli Dati: le informazioni relative alla tracciabilità del Dato (inserimento, modifica, cancellazione) vengono gestite con le stesse modalità del Dato cui si riferiscono.

Per quanto riguarda l'accesso ai servizi *Internet*, il S.I. garantisce la custodia dei file "*log*" per un perido di sei mesi, ove il tempo non sia diversamente indicato da fonti normative o regolamentari (per esempio di AgID).

Le registrazioni potranno essere utilizzate per finalità statistiche e di valutazione della qualità in riferimento a taluni servizi erogati, esclusivamente da parte di personale di ASP (o formalmente delegato) ed esclusivamente in formato anonimo e/o aggregato.

19.11 Comunicazione e diffusione

I Dati relativi all'utilizzo degli strumenti informatici sono trattati esclusivamente dagli operatori del S.I,. per le finalità indicate al punto precedente.

In applicazione delle procedure e delle disposizioni aziendali, in particolare in materia disciplinare, i *log* potranno essere oggetto di comunicazione ai soggetti aventi funzioni ispettive e di controllo all'interno dell'Azienda e, laddove ne ricorrano i presupposti di legge, alla Autorità Giudiziaria.

20. *Focus*: utilizzo dei mezzi di informazione e dei *social media*

Nell'ambito del generale dovere del dipendente pubblico di uniformare il proprio comportamento ai principi di diligenza, lealtà, imparzialità e buona condotta, egli è tenuto ad astenersi da qualsiasi intervento, dichiarazione, commento, diretto e/o indiretto, che possa nuocere al prestigio e/o al decoro e/o all'immagine dell'Azienda e/o della Pubblica Amministrazione in generale: pertanto anche nell'utilizzo dei propri *account* di *social media* e similari ed equivalenti, l'Utente utilizza ogni cautela affinché la proprie dichiarazioni e opinioni e/o giudizi su fatti, cose e/o persone non siano in alcun modo attribuibili, direttamente e/o indirettamente ad ASP o alla Pubblica Amministrazione in generale.

21. L'accessibilità

21.1. Premessa

Per *Accessibilità* s'intende la capacità dei sistemi informatici di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

L'Agenzia per l'Italia Digitale (AgID) promuove e favorisce la diffusione dell'accessibilità degli strumenti informatici all'interno della pubblica amministrazione in relazione alle disposizioni della normativa vigente.

La legge di riferimento per l'accessibilità digitale è la Legge n. 4 del 9 gennaio 2004 che ha attribuito ad AgID numerosi compiti, tra i quali:

- vigilare sull'attuazione della stessa Legge;
- fornire assistenza alla P.A. per l'applicazione della normativa vigente;
- emanare regole tecniche, circolari e linee guida in materia di accessibilità degli strumenti informatici;
- monitorare i siti *web* e le applicazioni mobili della P.A.;
- relazionare periodicamente la Commissione europea sugli esiti di monitoraggio;
- divulgare i temi dell'accessibilità nella P.A.

Nel 2018, con il Decreto legislativo n. 106 che modifica e aggiorna la Legge n.4/2004, l'Italia ha recepito la Direttiva UE 2016/2102, rivolta a migliorare l'accessibilità dei siti *web* e delle *app* mobili nel settore pubblico di ciascun Stato Membro.

In attuazione della Direttiva europea AGID ha emanato le *Linee Guida sull'Accessibilità degli strumenti informatici*[31], in vigore dal 10 gennaio 2020, che indirizzano la P.A. all'erogazione di servizi sempre più accessibili.

21.2. L'accessibilità in ASP Città di Bologna

ASP promuove e favorisce la diffusione dell'accessibilità degli strumenti informatici all'interno dell'Azienda in relazione alle disposizioni della normativa e delle indicazioni di AgID.

In particolare:

a) pubblica annualmente entro il 31/3 i propri obiettivi di accessibilità sul proprio sito e nell'apposita sezione predisposta da AgID;

b) rende conforme il proprio sito *web* e le proprie *app* ai requisiti di accessibilità entro i tempi previsti dalla normativa, in particolare con la pubblicazione annuale della propria *dichiarazione di accessibilità* sul proprio sito e nell'apposita sezione di AgID;

c) promuove la formazione interna sui temi inerenti all'accessibilità;

d) fornisce gli strumenti informatici necessari per garantire l'accessibilità, sia con progetti autonomi (esempio: l'adattamento continuo dei programmi informatici utilizzati in Azienda), sia su richiesta specifica di singoli utenti interessati (esempio: fornitura di *monitor* che consentano una lettura facilitata, cuffie, tastiere *braille* per posto operatore *ecc.*).

22. Responsabilità disciplinare

Il presente Regolamento dovrà essere osservato da ogni dipendente dell'Azienda, con la piena consapevolezza che eventuali violazioni dello stesso potranno fondare motivo di contestazione disciplinare.

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile:

- nei confronti del personale dipendente nelle forme del procedimento disciplinare con conseguente applicazione dei provvedimenti disciplinari e risarcitori previsti dalla normativa vigente applicabile (C.C.N.L., Codice disciplinare e dal Codice di Condotta dei dipendenti delle pubbliche amministrazioni, Codice Aziendale, *ecc.*),
- nei confronti dei collaboratori, consulenti, agenti e incaricati esterni a qualsivoglia titolo, verificata la gravità della violazione contestata, con la risoluzione o il recesso dal contratto a essi relativo nonché con tutte le correlate azioni civili e penali consentite.

[31] https://www.agid.gov.it/it/design-servizi/accessibilita/linee-guida-accessibilita-strumenti-informatici

23. Osservanza delle disposizioni in materia di *Privacy* (GDPR)

È obbligatorio attenersi alle disposizioni in materia di *Privacy*:

- di cui normativa in generale applicabile (GDPR, *Codice Privacy*, *ecc.*);
- in ottemperanza al presente Regolamento per l'utilizzo delle risorse informatiche di ASP;
- nel rispetto delle misure di sicurezza individuate dal Titolare del Trattamento e di cui anche al presente Documento;
- in ottemperanza alle direttive e istruzioni operative ricevute;
- in conformità con gli obblighi connessi e discendenti dal rapporto di contrattuale (contratto di lavoro, collaborazione, *ecc*. in essere con ASP) e dalle conseguenti mansioni/prestazioni rese;

come peraltro anche richiamate nella lettera di designazione a Incaricato del Trattamento dei Dati/soggetto terzo.

Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, II° c, della Legge n.300/1970.

Pertanto, come già espresso *sub* "Premesse" le informazioni raccolte come da presente Regolamento non sono utilizzate da ASP per finalità di controllo: invero, non sono installati o configurati sui sistemi informatici in uso agli utenti apparati *hardware* o strumenti *software* aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori, bensì unicamente l'espletamento di verifiche di sicurezza e prestazionalità del proprio sistema informatico e relative dotazioni[32].

Sul tema, peraltro, si rappresenta che qualora ASP necessitasse a fini quali a esempio: la sicurezza del lavoro, la tutela del patrimonio Aziendale, esigenze organizzative e/o produttive, il Titolare provvederà conformemente a quanto disposto dall'art.4 c.1 L. 300/1970 (ed ev. succ. mod. e int.) ossia che "*gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori […]possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. […] In mancanza di accordo, gli impianti e gli strumenti […] possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. […]*".

Sempre sul punto, poi, si precisa ulteriormente che la possibilità di cui al precedente paragrafo "*non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*"[33] e che, tuttavia, le informazioni raccolte con entrambe le modalità, "*sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196" e succ. mod. e int.*"[34].

Infine, in relazione all'accesso ai Dati trattati dall'Utente, si rinvia alle prescrizioni sovra esposte.

24. Aggiornamento e Revisione

Il presente Regolamento è soggetto periodicamente a revisione in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità tecniche: l'ultima versione sarà sempre consultabile sul sito *Intranet* Aziendale e sul Portale del Dipendente, nell'apposita sezione dedicata.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dai soggetti competenti del caso, di volta in volta individuati come da Organigramma Aziendale.

[32] Fermo restando che in caso di illeciti effettivi l'Ente potrà attivare i c.d. "controlli difensivi" che esulano dalla disciplina dello Statuto dei lavoratori.
[33] Art. 4 c.2 L.300/1970.
[34] Art. 4 c.3 L. 300/1970.

Sarà cura di ciascun Utilizzatore accertarsi se siano state pubblicate nuove versioni del presente Regolamento e conseguentemente conformare la propria condotta lavorativa a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività.

25. Rinvio

Per tutto quanto non espressamente previsto dal presente Regolamento si rinvia all'interezza delle prescrizioni previste dalla normativa tutta vigente e applicabile in materia.

Allegato 1: ***Elenco applicativi di base e specifici autorizzati in uso in ASP Città di Bologna*.**

In questo elenco sono riportati i programmi di cui è consentito l'utilizzo sui sistemi Aziendali; il presente Allegato costituisce parte integrante del Regolamento ed è aggiornato al 20.07.2023: eventuali ulteriori modifiche e integrazioni saranno recepite in nuovo elenco che sarà pubblicato e reperibile sia presso il sito *internet* istituzionale (https://aspbologna.acmecms.it/it/regolamenti), nella pagina dedicata, che sull'*intranet* aziendale (https://intranet.aspbologna.it/intranet/index.php?option=com_content&view=category&id=476&Itemid=749).

L'elenco in questo allegato costituisce anche la whitelist Aziendale come previsto dalla ABSC_ID 2.1.1 di cui anche alla Circolare AgID 2/2017

Sistemi gestionali

#	Produttore o fornitore	Nome commerciale / Sistema	Breve descrizione
1	Autodesk	Autocad LT	Software disegno tecnico e progettazione
2	Autogestito	Piattaforma Joomla	Gestione sito Internet e Intranet
3	CBA	Gestione turni	
4	Dedalus (Softech)	Garsia	Modulo gestione rendicontazioni assistenza domiciliare
5	DigitalPA	Gestione segnalazioni (whistleblowing)	Gestione segnalazioni ex L. n° 179/2017del 15/11/2017
6	Engineering (IdeaRe)	Ref	Gestione patrimonio immobiliare
7	GPI / (Infoline)	Jobtime, Gestione Risorse Umane	Suite gestionale composta di vari moduli applicativi
8	GPI	Eusis	Suite gestionale sistema amministrativo contabile
9	GPI	Domus	Gestione patrimonio immobiliare
10	GPI	Gestione ospiti	Gestione ospiti reparti, centri diurni, diete
11	Newbit / Dialog / (DWH) Engineering	Gestione processi	Varie procedure gestione SPRAR, Concorsi, Fornitori / Clienti WEB, Datawarehouse
12	Newteam	Tesis	Gestione richieste forniture e interventi
13	Software Uno (Zucchetti)	Lapis	Piattaforma documentale (Protocollo, delibere, determine, pubblicazione trasparenza), Accesso civico
14	Nutrium	Metadieta	Applicativo per nutrizionisti
15	IdeaRE	Reftree	Gestione patrimonio immobiliare
16	CBA – Zucchetti Health	Cartella socio sanitaria	Gestione cartella ospiti e CD

Software di base, infrastrutturali, utilità

#	Produttore o fornitore	Nome commerciale / Sistema	Breve descrizione
1	Filemaker	Filemaker server	Sviluppo database
2	Google	Chrome e Workspace	Browser web e strumenti automazione d'ufficio
3	Microsoft	Windows server e client	Sistemi operativi server e client in tutte le versioni
4	Microsoft	Office	Varie versioni

5	Microsoft	Windows Media Player	
4	Mozilla	Firefox	Browser web
4	Symantec	Gestione backup	
5	TeamViewer	TeamViewer	Software accesso remoto
6	Trend Micro	Enterprise Security for Endpoints Light	Antivirus endpoint
7	VLC	Media player	
8	OpenLicence	Open Office	
9	Adobe	Reader	
10	OpenLicence	7-zip	
11	Oracle	Java	
12	Uvnc/Teamviewer	VNC / UltraVNC / Teamviewer	

Bologna, 23 Luglio 2024

L'Amministratore Unico
STEFANO BRUGNARA