SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Ferrara

Università degli Studi di Ferrara

FRONTESPIZIO DELIBERAZIONE

AOO: AOU_FE

REGISTRO: Deliberazione

NUMERO: 0000003

DATA: 13/01/2022 17:28

OGGETTO: approvazione del “Disciplinare sull’utilizzo dei Sistemi Informatici Aziendali”.

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Bardasi Paola in qualità di Commissario Straordinario
Con il parere favorevole di Longhitano Elda - Sub Commissario Sanitario
Con il parere favorevole di Gamberini Maria - Sub Commissario Amministrativo

Su proposta di Barbara Paltrinieri - Affari Istituzionali e Segreteria Generale che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [04-05]

DESTINATARI:

- Collegio sindacale
- DIREZIONE GESTIONE OPERATIVA
- Gest.Conces.Serv.Generali E Commer. Cona
- Direzione Att. Amm.Ve Di Presidio
- Direzione Delle Professioni
- Ufficio Legale
- Medicina Legale ospedaliera
- Dir. Amm.Ne Risorse Econom Finanziarie
- Programmazione E Controllo Di Gestione
- Servizio interaziendale Formazione e Aggiornamento
- Servizio Comune Gestione del Personale
- Servizio Comune Economato e Gestione Contratti
- Servizio Comune Tecnico e Patrimonio
- Servizio Assicurativo Comune
- Ingegneria Clinica
- Fisica Medica
- Servizio Tenuta Protocollo Informatico

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000003_2022_delibera_firmata.pdf	Bardasi Paola; Gamberini Maria; Longhitano Elda; Paltrinieri Barbara	6F2410B9FEEBB2E39C1F189AE2248EED160676915B69DBE28A26BBD528062FF8
DELI0000003_2022_Allegato1.pdf:		32346CE6A6785384B0114DF5A028C2FB67E851A2DD167D2B1A30C498B790C102

DELIBERAZIONE

OGGETTO: approvazione del “Disciplinare sull’utilizzo dei Sistemi Informatici Aziendali”.

IL COMMISSARIO STRAORDINARIO

Vista la proposta di adozione dell’atto deliberativo presentata dal Dirigente Responsabile della Struttura Semplice Affari Istituzionali e Segreteria Generale, di cui è di seguito trascritto integralmente il testo:

“”

Premesso che:
- la disciplina introdotta dal Regolamento (UE) 2016/679 (d’ora in poi RGPD), è direttamente applicabile in tutti gli Stati membri dell’Unione Europea a partire dal 25 maggio 2018;
- la principale novità introdotta dal Regolamento consiste nell’affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti, e consegna la protezione dei dati nelle mani del Titolare del trattamento il quale, grazie al principio di responsabilizzazione (“accountability”), potrà, nei limiti e dentro i parametri delineati dal RGPD, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento dei dati personali;

Dato atto, peraltro, che l’implementazione del “sistema privacy” delineato dal RGPD implica la necessità di generare nell’organizzazione la piena consapevolezza del rischi inerenti ai trattamenti dei dati e le responsabilità connesse, nonché l’affermazione di una cultura della protezione dei dati quale parte integrante della vita lavorativa dell’organizzazione, con particolare attenzione ai dati sanitari (ivi compresi i dati biometrici e genetici), nonché ai cosiddetti dati sensibili sotto il profilo dei diritti e delle libertà fondamentali dell’individuo;

Richiamata la vigente delibera n. 45 del 27/02/2020 recante: “Regolamento recante il sistema di gestione dei dati personali nell’Azienda Ospedaliero-Universitaria di Ferrara “Arcispedale S. Anna” in applicazione del regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati)";

Dato atto che il Garante per la Protezione dei Dati Personali, con Del. n. 13 del 1° marzo 2007, ha approvato le “ *Linee guida del Garante per posta elettronica e internet*” nell’ambito delle quali, ai sensi degli artt. 24 e 154, comma 1, lett. b) e c) dell’allora vigente Codice in materia di protezione dei dati personali (d. lg.30 giugno 2003, n.196), ha:

- prescritto ai datori di lavoro privati e pubblici di adottare ogni misura necessaria a garanzia degli interessati riguardante l’onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

- indicato ai medesimi datori di lavoro, le linee guida a garanzia degli interessati per ciò che riguarda: **(a)** l'adozione e la pubblicizzazione di un disciplinare interno; **(b)** l'adozione di misure di tipo organizzativo affinché, segnatamente: si proceda ad un'attenta valutazione dell´impatto sui diritti dei lavoratori; si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l´utilizzo della posta elettronica e dell´accesso a Internet; si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi; l'adozione di misure di tipo tecnologico, sia **rispetto alla "navigazione" in Internet** (individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa; la configurazione di sistemi o l´utilizzo di filtri che prevengano determinate operazioni; il trattamento di dati in forma anonima o tale da precludere l´immediata identificazione degli utenti mediante opportune aggregazioni; l´eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza; la graduazione dei controlli), sia **rispetto all´utilizzo della posta elettronica (**messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali; eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato; messa a disposizione di ciascun lavoratore di apposite funzionalità che consentano di inviare automaticamente messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto presso la quale opera il lavoratore assente; consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica l´interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare quelli ritenuti rilevanti; inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l´eventuale natura non personale del messaggio); la graduazione dei controlli.
- vietato ai datori di lavoro privati e pubblici, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori, svolti in particolare mediante: **(a)** la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail; **(b)** la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore; **(c)** la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo; **(d)** l' analisi occulta di computer portatili affidati in uso;

Dato atto che detta deliberazione del Garante per la protezione dei dati personali è stata recepita, in ambito Aziendale, con il "Disciplinare sull'utilizzo di Internet e posta elettronica dell'Azienda Ospedaliero-Universitaria di Ferrara" approvato con delibera dell'intestata Azienda n. 117 del 24/06/2015;

Ritenuto, anche alla luce della successiva decisioni del Garante per la protezione dei dati personali (v., fra gli altri, il provv. n. 91 del 19 maggio 2020 -doc. web 9441579- o l'ordinanza-ingiunzione n. 115 del 2 luglio 2020 -doc. web 9445180-), detta Deliberazione sia da considerarsi tutt'ora vigente, sia alla luce di quanto dispongono gli articoli 13, 14, 24 e 25 del RGPD, sia in considerazione della persistenza dei poteri prescrittivi del Garante stesso, di cui all'art. 58 del RGPD medesimo;

Ritenuto, in ogni caso, che l'aggiornamento del Disciplinare, oltre che finalizzato a regolamentare le attività di trattamento svolte dai soggetti autorizzati per il tramite dei Sistemi Informatici e Informativi Aziendali, è finalizzato anche ad informare gli stessi del trattamento dei loro dati personali;

Dato atto che, nello svolgimento delle attività conferite ai sensi dell'art. 39 lett. a) e b) del Regolamento UE 2016/679, il DPO ha avviato una serie di incontri e confronti con i Direttori, o delegati, del Servizio Comune ICT, del Servizio Comune Gestione del Personale, dell'Area Comunicazione e Accoglienza e degli Affari Istituzionali e di Segreteria ai fini dell'aggiornamento del predetto "Disciplinare sull'utilizzo di Internet e posta elettronica dell'Azienda Ospedaliero-Universitaria di Ferrara" approvato con la richiamata delibera n. 117 del 24/06/2015, anche allo scopo di adeguarlo alla prassi del Garante, all'evoluzione tecnologia e alle nuove disposizioni di cui al RGPD;

Dato atto che, nel contesto degli incontri e confronti di cui al punto precedente, si è ritenuto di far confluire nel rinnovo del predetto disciplinare anche il "Regolamento aziendale per l'assegnazione di utenze della telefonia mobile" approvato con la medesima delibera n. 117 del 24/06/2015, in considerazione dell'affinità, derivante dallo stato della tecnica, tra le utenze di telefonia mobile e i Sistemi Informatici Aziendali;

Dato atto che il presente provvedimento risponde ai principi della legittimità, opportunità e convenienza;

" "

Attesa la rappresentazione dei fatti e degli atti riportati dal Dirigente Responsabile della Struttura Semplice Affari Istituzionali e Segreteria Generale e ritenuto di adottare il presente provvedimento, approvando il Disciplinare sull'utilizzo dei Sistemi Informatici Aziendali" allegato quale parte integrante e sostanziale del presente provvedimento, il quale sostituisce integralmente il precedente Regolamento e il precedente Disciplinare approvati con delibera n. 117 del 24/06/2015;

Delibera

1) di provvedere all'adozione del "Disciplinare sull'utilizzo dei Sistemi Informatici Aziendali" allegato quale parte integrante e sostanziale del presente provvedimento il quale sostituisce integralmente il precedente Regolamento e il precedente Disciplinare approvati con delibera n. 117 del 24/06/2015;

2) di trasmettere il presente provvedimento ai Direttori delle Strutture aziendali al fine della massima divulgazione all'interno delle Strutture dirette anche attraverso la pubblicazione sul sito web aziendale;

3) di dare mandato al Servizio Comune Information & Communication Technology di consegnare il Disciplinare unitamente ai Servizi Informatici Aziendali ivi disciplinati;

4) di prevedere la pubblicazione del presente provvedimento nella sezione "Atti amministrativi generali" e nella Sezione "Privacy" di "Amministrazione Trasparente" del sito istituzionale di questa Amministrazione;

5) di procedere alla pubblicazione del presente provvedimento all'Albo Elettronico, ai sensi dell'art. 32 della L. 69/2009 e s.i.m., per quindici giorni consecutivi;

6) di dichiarare il presente provvedimento esecutivo dal giorno della pubblicazione.

Responsabile del procedimento ai sensi della L. 241/90:
Barbara Paltrinieri

DISCIPLINARE SULL'UTILIZZO DEI SERVIZI INFORMATICI AZIENDALI

Sommario

Premessa.

Nel pieno rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento al diritto alla protezione dei dati personali (art. 1, comma 2, del Regolamento UE 2016/679) l'**Azienda Ospedaliero-Universitaria di Ferrara**, di seguito denominata Azienda, adotta il presente "Disciplinare sull'utilizzo dei Servizi Informatici Aziendali".

La normativa e gli atti di riferimento del presente Regolamento sono:

a) REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito denominato "RGPD";
b) il D.Lgs 30 giugno 2003, n. 196 e successive modificazioni e integrazioni, recante Codice in materia di Protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/456/CE, di seguito denominato "Codice";
c) Il D.Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni, recante Codice per la amministrazione digitale", di seguito denominato "CAD";
d) Il Provvedimento a carattere generale del Garante per la protezione dei dati personali dell'1/03/2007 ad oggetto: "Lavoro: le linee guida del Garante per posta elettronica e internet", pubblicato in G.U. n° 58 del 10/03/2007, di seguito denominato "Linee Guida";
e) l'art. 2, comma 595, della legge 24 dicembre 2007, n. 244, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)";
f) la legge 20 maggio 1970, n. 300 e successive modifiche ed integrazioni, recante "Statuto dei lavoratori", di seguito denominato "Statuto";
g) la Direttiva 26 maggio 2009 n. n. 2 del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri, di seguito denominata "Direttiva".

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate. Le proposte verranno esaminate dall'ICT. Il presente "Disciplinare" è soggetto a revisione con frequenza almeno biennale da parte del Servizio Comune ICT.

Art. 1. Oggetto.

1. Il "Disciplinare" ha per finalità di stabilire le norme per l'accesso e l'utilizzo dei seguenti servizi dell'Azienda:

1) Posta elettronica,
1) Rete internet,
2) Computer aziendali,
3) Utenza di telefonia mobile,

di seguito indicati nel loro complesso come “Servizi informatici Aziendali” (d'ora in poi SIA), i quali sono altresì regolamentati anche da eventuali altre disposizioni quali, a mero titolo esemplificativo, regolamenti, linee guida, disciplinari, istruzioni operative sull’accesso e l’uso di specifiche risorse informatiche o informative (ad esempio il REGOLAMENTO PER LA DISCIPLINA DEL LAVORO AGILE E TELELAVORO PER IL PERSONALE DEL COMPARTO E DELLE AREE DIRIGENZIALI e/o altre disposizioni adottate per l’uso di applicazioni, portali, software di ingegneria clinica ed altri)

2. Il presente “Disciplinare” è rivolto ai dipendenti dell'Azienda e loro equiparati, ivi comprese le altre figure, pur non dipendenti, comunque autorizzate al trattamento dei dati (es. collaboratori esterni, fornitori, ospiti, ecc.) alle quali, al momento dell’incarico, deve essere fornito il presente Disciplinare, anche attraverso l’indicazione della pagina del sito Internet aziendale nel quale è pubblicato. In ogni caso, ai sensi dell’art. 7 dello Statuto, il presente Disciplinare è oggetto di affissione in modalità telematiche, mediante pubblicazione nella Sezione Privacy del sito internet aziendale.

3. È fatto obbligo a tutti gli Utenti di osservare le disposizioni portate a conoscenza con il presente Disciplinare, le cui disposizioni hanno valore di “norme disciplinari” ai sensi dell’art. 7 dello Statuto

4. Il mancato rispetto o la violazione delle regole di cui al presente Disciplinare da parte del personale dipendente, a prescindere dalle misure di tipo preventivo eventualmente applicabili ed applicate, è in ogni caso perseguibile con i provvedimenti disciplinari previsti dal vigente CCNL applicabile all’Utente che ha commesso la violazione, nonché con tutte le azioni, anche di tipo risarcitorio, in ambito civile, penale ed amministrativo. La violazione delle disposizioni del presente Disciplinare, pertanto, verranno segnalate dal Referente Interno all’Ufficio Procedimenti Disciplinari.

5. Nei confronti del personale non dipendente, autorizzato a prestare la propria attività lavorativa all’interno dell’Azienda, o comunque autorizzato al trattamento dei dati, in caso di violazioni del presente Disciplinare, saranno applicabili le misure preventive della revoca delle assegnazione e/o dell’autorizzazione all’uso dei SIA e, laddove tale uso sia indispensabile per lo svolgimento dei compiti affidati, misure ulteriori che possono comportare anche la risoluzione del rapporto contrattuale in corso, nonché, in presenza dei necessari presupposti, il ricorso alle azioni amministrative e/o giudiziarie, anche di tipo risarcitorio, necessarie ai fini della tutela dei diritti e degli interessi dell’Azienda.

6. Il presente “Disciplinare”, laddove comporti il trattamento di dati personali degli Utenti, ha anche valore di “informativa” ai sensi degli articoli 13 e 14 del RGPD.

7. Nel presente “Disciplinare” i termini di seguito elencati hanno le correlate definizioni:

a) ICT: Servizio Comune ICT;
b) REFERENTE INTERNO e/o REFERENTE PRIVACY: si intende il Referente di cui all’art. 4 del REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI DELL’AZIENDA OSPEDALIERO-UNIVERSITARIA DI FERRARA pubblicato nella

Sezione Privacy del sito istituzionale e, quindi, il dirigente responsabile di struttura complessa Ospedaliera e Universitaria, il dirigente responsabile di struttura semplice dipartimentale, di programma assistenziale, il dirigente responsabile di struttura semplice, nonché il responsabile delle unità organizzative in staff con la Direzione Generale;

c) INGEGNERIA CLINICA: Servizio Comune di Ingegneria Clinica;
a) UTENTE: persona autorizzata all'utilizzo dei SIA;
b) USERID e/o CODICE DI IDENTIFICAZIONE PRSONALE: il codice assegnato all'utente per l'accesso ai SIA;
c) BLACK-LIST: elenco dei siti non accessibili agli utenti;
d) CATENA DI S. ANTONIO: invio di messaggi di posta elettronica che istighino il destinatario a propagare i messaggi ricevuti ad una pluralità di destinatari, senza attinenza con l'attività lavorativa;
e) INDIRIZZO IP: numero che identifica univocamente un dispositivo collegato ad una rete informatica;
f) INTERNET PROVIDER: azienda che fornisce alle Aziende il canale di accesso alla rete Internet;
g) LOG: registrazione elettronica automatica generata da applicazioni o dispositivi, riguardante informazioni sulle attività eseguite all'interno degli impianti aziendali;
h) MAIL SPAMMING: invio massivo di messaggi di posta elettronica non desiderati e diretti ad una pluralità di destinatari, aventi generalmente contenuto commerciale o comunque non attinente l'attività lavorativa;
i) POSTAZIONE DI LAVORO: personal computer (PC), o altro idoneo dispositivo, collegabile alla rete aziendale tramite il quale l'utente accede ai servizi.

Art. 2. Autorizzazione al trattamento dei dati personali.

1. I SIA sono strumenti di lavoro forniti dall'Azienda, che ne fissa le modalità di utilizzo che gli utenti sono tenuti ad osservare scrupolosamente.

2. Gli utenti sono autorizzati, ai sensi del RGPD, al trattamento dei dati ai quali hanno accesso o che sono trattati mediante i SIA secondo le disposizioni di cui al REGOLAMENTO RECANTE IL SISTEMA DI GESTIONE DEI DATI PERSONALI pubblicato nella Sezione Privacy del sito istituzionale.

3. Gli utenti, in ogni caso, possono trattare i dati limitatamente alle operazioni indispensabili per le finalità per i quali sono stati raccolti e nei limiti delle funzioni loro attribuite, e comunque nel rispetto dei principi di pertinenza e non eccedenza stabiliti dalle norme vigenti.

Art. 3. Identificazione dell'utente per l'accesso ai servizi.

1. L'utilizzo dei SIA richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) ed una parola chiave segreta (password).

2. L'Azienda si riserva, a seguito di evoluzione delle tecnologie, di introdurre, anche solo in particolari contesti, sistemi di autenticazione "forte", basati, ad esempio, su smart card o caratteristiche biometriche, nel rispetto delle normative vigenti.

3. Per accedere ai SIA, un nuovo utente dovrà fornire i propri dati identificativi, prendere visione del presente regolamento e compilare e sottoscrivere in forma completa in ogni sua parte i moduli di richiesta di abilitazione di volta in volta predisposti e disponibili sulla intranet aziendale.

4. Il modulo dovrà essere consegnato all'ICT, timbrato e firmato dal Referente Interno della struttura alla quale l'utente appartiene. L'incompleta compilazione e autorizzazione del modulo sopra citato ne comporterà l'automatico annullamento.

5. L'Azienda si riserva, a seguito di evoluzione della tecnologia, di sostituire la modulistica cartacea con sistemi di autorizzazione elettronica.

6. La password non potrà essere ceduta a terzi neppure temporaneamente, dovrà essere mantenuta segreta e dovrà essere obbligatoriamente modificata dall'utente in ogni caso in cui egli abbia fondati sospetti che la segretezza della password sia venuta meno.

7. Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi. L'utente non deve lasciare incustodita o facilmente accessibile la postazione di lavoro una volta collegata al sistema, e deve disattivare la connessione qualora si debba allontanare.

8. L'utente non deve rendere accessibili in alcun modo le informazioni concernenti la propria password.

9. L'userid, alla cessazione del rapporto di lavoro, viene archiviata e non potrà essere riassegnata ad altro utente se non all'utente stesso in caso di costituzione di nuovo rapporto di lavoro. Non sono previsti codici di accesso anonimi, salvo nei casi in cui sia prevista una successiva procedura di identificazione personale per l'accesso alle procedure e/o ai dati veri e propri.

10. L'utente deve conservare la password con la massima riservatezza e con la massima diligenza.

11. La password:

    a) non deve essere banale né contenere riferimenti riconducibili all'utente;
    b) dovrà essere lunga almeno 8 caratteri i quali dovranno necessariamente comprendere lettere minuscole, lettere maiuscole, numeri, caratteri speciali;
    c) dovrà essere modificata dall'utente al primo utilizzo e, successivamente, almeno ogni tre mesi e non potrà essere riutilizzata per i sette cambi successivi.

12. Alla scadenza dei tre mesi, nel caso in cui l'utente non avesse provveduto a modificare la propria password, la sua abilitazione verrà sospesa. L'utente avrà ancora due mesi per riattivare il proprio profilo semplicemente cambiando la password con le modalità opportune e in modo autonomo. Alla scadenza di questi ulteriori due mesi, il codice di identificazione personale (userid) verrà disattivato.

13. Nel caso in cui l'utente dimentichi la propria password è disponibile un link all'interno dell'area dipendenti del sito istituzionale per il recupero automatico. Nel caso di problemi nell'utilizzo della procedura automatica, per riottenere l'accesso ai servizi, l'utente dovrà inviare una richiesta di reimpostazione della password al Servizio Comune ICT, firmata e con allegata una fotocopia di un documento di identità o del tesserino di riconoscimento aziendale o presentandosi personalmente presso il medesimo ICT.

14. Nel caso di disattivazione del codice di identificazione personale, per riottenere l'accesso ai servizi l'utente dovrà compilare nuovamente il modulo "Richiesta di abilitazione ai servizi informatici aziendali" e consegnarlo all'ICT, firmato dal Responsabile della struttura organizzativa a cui l'utente appartiene.

15. Dopo sei mesi di non utilizzo dei servizi, la userid e la password verranno automaticamente disattivati. Decorso tale periodo di tempo l'utente dovrà chiederne la riattivazione all'ICT.

Art. 4. Finalità e limitazioni d'uso.

1. L'accesso ai SIA e alla navigazione in Internet è da intendersi consentita all'esclusivo scopo lavorativo e può pertanto essere effettuato nei limiti di quanto necessario per lo svolgimento della propria attività e delle proprie mansioni, essendo quindi vietato l'uso e la navigazione in Internet per motivi diversi da quelli necessari per l'espletamento delle proprie mansioni.

2. È vietato l'uso dei SIA, ivi compresa la navigazione in Internet, nei seguenti casi:

   a) per l'upload o il download di programmi per elaboratore gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http;
   b) per transazioni finanziarie ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati;
   c) per ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
   d) per la partecipazione a Forum non professionali, l'utilizzo di chat line e social network, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Referente;
   e) per l'utilizzo di applicativi per l'ascolto della musica e/o la visione di video su siti se non espressamente autorizzati dal Referente in quanto necessario per lo svolgimento delle proprie mansioni per l'utilizzo di procedure aziendali con modalità e finalità non attinenti ai propri doveri d'ufficio;
   f) per ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
   g) per trasferire sulla postazione dell'utente programmi e/o file di dati relativi a progetti od obiettivi estranei all'utente o per finalità personali (es., file il cui contenuto sia protetto da diritto d'autore);
   h) per ricerche e/o consultazioni, all'interno dell'orario di lavoro, in maniera ripetuta e unicamente per scopi personali, di siti il cui contenuto informativo non sia attinente con l'attività lavorativa dell'utilizzatore;

i) per ricerche e/o consultazioni palesemente incompatibili con i fini istituzionali dell'Azienda.

3. È comunque vietato l'uso dello strumento nei casi configurati dalla normativa vigente come reato, in particolare:

   a) diffusione di virus, “cavalli di troia” o altri programmi la cui azione consista nel sabotaggio, distruzione, alterazione o visione del contenuto informativo delle postazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l’obiettivo sia all'esterno della rete aziendale;
   b) per attività di furto di dati aziendali o di altri utenti, organismi e/o aziende;
   c) per attività di hackeraggio e pirateria informatica in generale.

4. È consentito agli utenti il salvataggio di documenti contenenti dati personali, nell’esclusivo caso in cui sia necessario per lo svolgimento delle proprie mansioni, nei soli SIA messi a disposizione dall’ICT. E’ quindi fatto divieto agli utenti di salvare documenti contenenti dati personali su supporti informatici personali non preventivamente autorizzati e/o consegnati dall’ICT.

Art. 5. Rilevazione statistica delle attività di accesso ad Internet.

1. Le operazioni di accesso ad Internet potranno essere memorizzate per finalità di sicurezza del sistema con la gradualità prevista dalla normativa vigente.

2. La rilevazione statistica delle attività avviene attraverso i file di “log” generati automaticamente dai sistemi.

3. La conservazione dei log avviene in conformità con la normativa vigente, o comunque sulla base di indicazioni operative del Direttore ICT, previo parere del Responsabile della Protezione dei Dati.

4. Non verranno estratte statistiche a livello individuale, bensì su base aggregata per area, settore o ufficio. In nessun caso i log del sistema generati sono usati come strumento di controllo dell'operato dell'utente. Da essi non è ricavabile alcuna informazione relativa al tempo trascorso nelle varie navigazioni dai singoli utenti.

5. I log potranno essere oggetto di provvedimenti dell'Autorità Giudiziaria e Amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo. A seguito di specifica richiesta da parte delle Autorità preposte essi verranno consegnati secondo le istruzioni ricevute da parte delle Autorità stesse.

Art. 6. Rilevazione statistica delle attività di accesso remoto alle postazioni di lavoro.

1. Gli strumenti di accesso remoto utilizzati dall’ICT, ai sensi dell’art. 4, comma 2 dello Statuto, non costituiscono in alcun modo controllo a distanza dell'attività del lavoratore.

2. Ogni accesso remoto da parte di personale tecnico autorizzato ad una stazione di lavoro avviene solo per finalità di assistenza tecnica, al fine di

aggiornare/ripristinare le condizioni di funzionamento ottimali e/o di installarne delle nuove.

3. Ogni accesso avviene dietro consenso dell'utente espresso mediante la pressione di un tasto (o mediante altre azioni che denotino volontarietà e consapevolezza degli utenti); ciò, quindi, implica la presenza dell'utente davanti al monitor che ha piena visione delle operazioni svolte dall'addetto all'assistenza remota e ha facoltà di interromperle in ogni istante.
4. L'accesso remoto alle postazioni è ammesso senza consenso dell'utente se esse si trovano in modalità disconnessa ("logout"), e in tal caso l'utente remoto accede al sistema con le proprie credenziali senza accedere ai contenuti dei profili personali degli utenti del PC.
5. Nel caso in cui, per problematiche tecniche urgenti ed improcrastinabili, si renda necessario accedere con le credenziali di uno specifico utente, e questi non sia disponibile, verrà resettata la sua password e lo stesso dovrà provvedere alla sostituzione della password al primo collegamento.
6. In questi particolarissimi casi l'ICT documenterà dettagliatamente ogni operazione effettuata con le credenziali dell'utente, ed informerà lo stesso con la massima tempestività. In nessun caso l'ICT è legittimato a chiedere all'utente la password di accesso, che comunque non è conosciuta dal personale tecnico.

Art. 7. Configurazioni hardware e software.

1. Le postazioni di lavoro utente vengono predisposte e configurate per il corretto uso dei SIA dall'ICT. L'utente si impegna a mantenere la corretta configurazione della postazione di lavoro che utilizza.
2. Le politiche relative ai software di gestione della sicurezza sono gestite centralmente e non è richiesta all'utilizzatore alcuna operazione manuale in merito.
3. Al fine di erogare in modo ottimale i servizi di manutenzione ai SIA, l'ICT, fermi restando gli obblighi previsti dalla normativa vigente, si riserva di installare software diagnostici che raccolgono informazioni tecniche e di configurazione dei dispostivi.
4. A tal fine, Le postazioni di lavoro sono normalmente configurate per consentire l'accesso dell'utente solamente in modalità non privilegiata. Nel caso in cui a causa di particolari requisiti tecnici si renda necessario elevare i privilegi informatici dell'utente, quest'ultimo è maggiormente tenuto a preservare la configurazione della propria macchina così come impostata dall'ICT.
5. Qualora durante un intervento di manutenzione, i tecnici ICT rilevino postazioni utente non conformi agli standard aziendali autorizzati, in mancanza di una specifica precedente deroga, gli stessi procederanno d'ufficio a ripristinare tali postazioni secondo gli standard definiti.
6. Nel caso in cui l'utente ritenga siano necessarie modifiche alla configurazione, ivi compresa l'installazione di nuovi programmi, dovrà formulare una richiesta

via mail all'ICT che provvederà ad autorizzarla o meno, in quanto ogni modifica implica potenziali ricadute sulle corrette funzionalità delle procedure aziendali.

7. L'utente è responsabile delle attrezzature informatiche a lui assegnate, anche temporaneamente, e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo ne! luogo di lavoro, soprattutto nel caso di attrezzature portabili.

8. I dispositivi portabili devono essere restituiti, al termine del periodo di utilizzo concordato, alla struttura che li ha assegnati.

Art. 8. Modalità di prestazione dei servizi.

1. L'Azienda si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità d'interromperli per le manutenzioni ordinarie o in caso di situazioni straordinarie (ad es. attacco informatico) che possano compromettere integrità, disponibilità e riservatezza dei dati aziendali.

2. Qualora possibile le interruzioni saranno preventivamente comunicate agli utenti.

3. Per migliorare la qualità o la sicurezza dei servizi e dei sistemi informatici attualmente predisposti, l'Azienda valuterà con attenzione eventuali osservazioni, suggerimenti e indicazioni che gli utenti faranno pervenire all'ICT.

4. L'operatività specifica del personale ICT, per la peculiare attività che svolge, è disciplinata nell'atto che lo autorizza al trattamento, ai sensi dell'art. 2-*quaterdecies* del Codice, in qualità di amministratore di sistema.

Art. 9. Backup e protezione dati particolari.

1. L'ICT provvede al salvataggio periodico delle banche dati prodotte dai Sistemi Informatici Centralizzati. La periodicità è indicata nelle Linee programmatiche aziendali sulla sicurezza dei dati adottate dal Direttore dell'ICT.

2. L'ICT rende disponibile una infrastruttura cloud a cui tutti gli utenti sono tenuti a collegarsi per registrare i propri documenti aziendali conservati nelle SIA. La capienza massima individuale, pari a 5GB, è incrementabile, su richiesta via mail all'ICT medesimo, in caso di necessità ulteriori. I dati registrati sulla predetta infrastruttura sono sottoposti a backup quotidiano a cura dell'ICT.

3. Gli utenti possono richiedere all'ICT la creazione di cartelle condivise tra più utenti. Gli utilizzatori della cartella condivisa dovranno utilizzarla in conformità alle normative vigenti, ai propri ambiti lavorativi nonché ai fini istituzionali dell'azienda. Tali cartelle verranno altresì inserite nei backup automatici.

4. È vietato memorizzare sui PC aziendali dati personali o sensibili estranei all'attività aziendale. Rimane comunque responsabilità dell'utente la cura e la protezione di eventuali file contenenti dati riservati e/o sensibili memorizzati sul proprio PC.

Art. 10. Pubblicazione di contenuti e realizzazione di siti personali.

1. E’ vietato all'Utente produrre, pubblicare o manutenere siti web diversi da quello ufficiale aziendale mediante la rete aziendale e/o i SIA, salvo specifica autorizzazione del Direttore Area Comunicazione.
2. È altresì vietato utilizzare il sito aziendale, anche mediante la pubblicazione o inserimento di link a siti esterni, per pubblicizzare e/o promuovere attività non confacenti o addirittura in concorrenza con le attività erogate dall'Azienda.
3. È diritto di ogni servizio chiedere di inserire uno spazio informativo (tecnicamente consistente in una o più “pagine”, collegate tra loro ed alla “home page” aziendale) sul sito aziendale, di cui è direttamente responsabile anche per il contenuto e la correttezza delle informazioni.
4. A tale proposito i servizi dovranno fare richiesta all'Area Comunicazione segnalando gli identificativi delle persone che potranno inserire informazioni sul sito e chi sarà il responsabile che ne autorizzerà la pubblicazione.
5. A tal fine l'Area Comunicazione provvederà a creare uno spazio web sul sito interno e/o sul sito pubblico, collegandolo alla pagina iniziale, o nella sotto-pagina eventualmente di riferimento.
6. L’ICT mette a disposizione il proprio supporto tecnico per la soluzione di eventuali problemi relativi all'applicazione delle procedure previste dal presente articolo, fatto salvo il fatto che l’inserimento e l'aggiornamento delle informazioni sono sempre a carico dei singoli servizi.
7. È fatto divieto agli Utenti di utilizzare il logo aziendale nei siti personali senza espressa autorizzazione del Direttore Area Comunicazione.
8. Si applicano in ogni caso le norme dei Codici deontologici professionali.
9. È vietato ospitare presso il server aziendale le pagine web di soggetti terzi (hosting) o concedere ad un Utente la possibilità di inserire un suo server all’interno dell’infrastruttura IT aziendale (housing), salvo specifica autorizzazione del Direttore ICT.

Art. 11. Connessione a provider diversi da quelli aziendali.

1. All’interno dell’azienda è vietato accedere con i SIA alla rete Internet tramite connessione diverse da quelle aziendali o da quelle autorizzate dall’ICT.
2. Il divieto si estende anche alla connessione tramite “internet key” o sistemi analoghi non forniti o non autorizzati dall’’ICT.
3. Qualora sia disponibile una connessione di rete aziendale, cablata o wireless, questa è da considerarsi fortemente prioritaria rispetto all'utilizzo di altri sistemi di connessione.
4. Nello specifico per le connessioni wireless vanno usate prioritariamente quelle rese disponibili direttamente dalle aziende sanitarie ferraresi (WiFi-Dati, AUSLFE, SIC, FUT).

Art. 12. Servizio di Posta Elettronica.

1. Il Servizio Informatico fornisce due distinte tipologie di account di posta elettronica:

   a) account di servizio o di gruppo, il cui nome richiama il servizio in cui lavora l'utente;
   b) account legati al nominativo dell'utente richiedente.

2. Al momento dell'assunzione o dell'instaurazione del rapporto di collaborazione, a qualsiasi titolo, con l'Azienda, su segnalazione del Servizio Comune Gestione del Personale, l'ICT fornisce a ciascun Utente l'account di cui alla predetta lett. b).

3. Gli utenti sono tenuti ad utilizzare, per le comunicazioni aziendali, esclusivamente gli indirizzi di posta elettronica creati sui domini aziendali, essendogli quindi fatto divieto di utilizzare l'indirizzo di posta elettronica personale.

4. Tutti i possessori di una casella di posta elettronica nominativa sono tenuti a consultare quotidianamente la propria corrispondenza. Le comunicazioni istituzionali si considerano recapitate con l'invio alle caselle istituzionali degli Utenti.

5. È vietato l'utilizzo dell'account di posta elettronica aziendale per attività estranee all'ambito lavorativo.

6. In caso di eventuali assenze programmate dell'utente (es. ferie, attività di lavoro fuori sede), al fine di garantire la funzionalità del servizio di posta elettronica aziendale, il sistema deve essere configurato in modo da inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto scelto dall'Utente, o altre utili modalità di contatto. Nel caso in cui l'Utente intenda avvalersi di questa funzionalità può, laddove non riesca a provvedere autonomamente, chiedere supporto all'ICT.

7. In caso di eventuali assenze non programmate (es. malattia), qualora l'Utente si trovi nell'impossibilità di attivare la funzionalità di risposta automatica, l'ICT potrà disporre direttamente, su richiesta del Referente Interno, l'attivazione di analoghi accorgimenti laddove ciò si rendesse necessario al fine di garantire la continuità dell'attività aziendale.

8. Qualora risulti indispensabile e/o indifferibile accedere alla casella email in dotazione all'Utente, per cause di forza maggiore derivanti da esigenze improrogabili legate alla continuità dell'attività lavorativa, ad esigenze di sicurezza ed operatività dello stesso sistema informatico, l'Azienda può accedere alla casella di posta elettronica aziendale assegnata all'Utente per il tramite di un collega indicato dall'Utente stesso, anche telefonicamente, ed estrarre copia dei messaggi attinenti l'attività lavorativa. In tutti i casi in cui si rendesse necessario accedere alla casella di posta elettronica aziendale per le predette attività, le contingenze non consentissero all'Azienda di raggiungere tempestivamente l'Utente per l'indicazione di un collega che vi proceda, l'accesso sarà consentito al Referente affinché lo stesso possa procedere, congiuntamente al supporto tecnico dell'ICT all'uopo incaricato, alla verifica del

contenuto dei messaggi di posta elettronica inviati e ricevuti per mezzo dell'account di posta elettronica. Effettuata la verifica il Referente provvederà ad inoltrare i messaggi di posta e relativi allegati, rilevanti ai fini della contingenza e della continuità dell'attività svolta dell'Utente. Le predette attività verranno documentate mediante annotazione che attesti le operazioni svolte, e ciò anche a mezzo email destinata all'Utente assente.

9. Nel caso venga disattivato l'indirizzo di posta elettronica aziendale, la casella ed il relativo contenuto, costituendo patrimonio aziendale, rimarranno nella piena disponibilità della stessa per un periodo di 6 mesi dalla risoluzione del rapporto lavorativo, dopo il quale i messaggi verranno cancellati, salvo che non sia necessaria la loro conservazione per l'esercizio del diritto di difesa dinanzi l'autorità giudiziaria o per altre indifferibili esigenze finalizzate a tutelare i diritti e le libertà fondamentali degli interessati.

Art. 13. Comunicazioni di massa.

1. Gli Utenti sono tenuti a segnalare all'ICT, mediante e-mail all'indirizzo security@ospfe.it, l'eventuale ricevimento di messaggi, sia da utenti interni che esterni, appartenenti ad una delle seguenti categorie:

   a) "mail spamming" e "catene di S. Antonio";
   b) aventi contenuto diffamatorio per l'Azienda od i suoi dipendenti;
   c) aventi contenuto moralmente deplorevole, scandaloso, propagandistico per correnti politiche o fazioni religiose;
   d) aventi contenuto non attinente l'attività lavorativa ed il cui ricevimento sia "non gradito" all'utente;
   e) aventi il fine di "intasare" le caselle di posta elettronica.

2. Le comunicazioni massive destinate contemporaneamente a tutte le caselle di posta aziendali, necessarie per comunicazioni che rivestono importanza per un congruo numero di utenti, potranno essere inviate esclusivamente dalla Segreteria Generale, dall'Area Comunicazione o dal Responsabile della Protezione dei Dati Personali. Gli Utenti che abbiano necessità di inviare comunicazioni massive sono tenuti ad inviarle ai predetti soggetti, specificando la ragione della rilevanza massiva, i quali avranno cura di autorizzarne e/o disporne la trasmissione.

Art. 14. Assegnazione delle utenze di telefonia mobile.

1. La rete di telefonia mobile Aziendale è gestita dall'ICT, che assegna le utenze di telefonia mobile secondo i criteri espressi nel presente articolo.

2. L'ICT assegna l'utenza di telefonia mobile in modalità fonia e/o dati costituita da un numero telefonico associato ad una scheda SIM e, se richiesto, da un telefono cellulare:

   a) al personale aziendale che, operando in pronta disponibilità, deve essere tempestivamente raggiungibile tramite un numero cellulare che gli permetta di effettuare immediatamente da remoto tutte le comunicazioni necessarie, per risolvere l'emergenza per cui sono stati interpellati.

b) al personale aziendale che svolge la propria attività sul territorio e che per servizio ha necessità di contattare ed essere contattato dall'ufficio centrale d'appartenenza, oppure che deve comunicare con ditte, Aziende od utenti che intrattengono rapporti con l'Azienda anche dall'esterno della propria sede di lavoro.
c) al personale Dirigente, che ha la necessità di essere raggiungibile o di raggiungere dall'esterno della propria sede di lavoro le altre Direzioni Aziendali e/o i propri collaboratori.

3. L'utenza è assegnata agli utenti che ne facciano richiesta utilizzando l'apposito modulo reperibile nella Intranet aziendale, motivata e firmata dal Referente interno, approvata dal Direttore di macrostruttura di appartenenza e può essere assegnata limitatamente alla scheda SIM o estesa all'apparecchio cellulare e può riguardare le seguenti tipologie di abilitazione:

a) abilitazione all'uso della fonia e degli sms verso le sole numerazioni aziendali fisse e mobili;
b) abilitazione all'uso della fonia e degli sms verso le sole utenze nazionali;
c) abilitazione all'uso della fonia e degli sms anche verso utenze internazionali;
d) abilitazione alle chiamate fonia personali;
e) abilitazione al traffico dati (associata o meno ad una abilitazione fonia esistente).

Art. 15. Obblighi e doveri dell'intestatario del telefono mobile.

1. L'utente a cui è assegnata un'utenza di telefonia mobile aziendale ne è direttamente responsabile in relazione al suo corretto utilizzo in termini di contenuti comunicati e/o trasmessi ed è pertanto tenuto a seguire puntualmente le seguenti indicazioni operative:

a) l'utenza di telefonia mobile è stata concessa in uso dall'Azienda per essere utilizzata esclusivamente per motivi di lavoro; può essere utilizzata anche a scopo personale solo nel caso in cui sia stata autorizzata e attivata la modalità di ripartizione del traffico telefonico tra pubblico e privato nella modalità contrattuale definita "Dual Billing", che, a seguito di sottoscrizione di un apposito contratto, consente la fatturazione diretta delle telefonate private all'assegnatario dell'utenza previo utilizzo di un apposito codice da selezionare in fase di chiamata;
b) il telefono cellulare, la scheda SIM ed ogni altro accessorio consegnato all'utente dovranno essere conservati con cura. Saranno restituiti, su richiesta del Direttore ICT, qualora l'attività lavorativa del dipendente non necessiti più di utenza mobile;
c) l'utenza di telefonia mobile dovrà essere sempre tenuta accesa durante l'orario di servizio; la segreteria telefonica dovrà essere usata solo ed esclusivamente quando il telefono non è raggiungibile dal segnale radio;
d) Il Referente Interno è tenuto a comunicare all'ICT ogni eventuale variazione avvenuta dopo l'assegnazione dell'utenza, come ad esempio il cambio di utilizzatore, di sede lavorativa, di recapiti telefonici, ecc.;
e) non è consentito attivare il trasferimento di chiamata;

f) è fatto divieto al personale di trasmettere, attraverso sistemi di messaggistica istantanea (es. WhatsApp, Telegram, Signal, ecc.) e/o di social network, dati personali di titolarità dell'Azienda;
g) fermo restando quanto previsto nell'alinea precedente, nel caso vengano costituiti, su base volontaria, gruppi di messaggistica (es. gruppi Whatsapp, gruppi Telegram, gruppi Facebook, ecc.) e/o di sociale network, gli stessi non potranno essere utilizzati per trasmettere informazioni di carattere personale;
h) la navigazione Internet, la gestione della posta elettronica e l'accesso remoto alle procedure aziendali sono sottoposti alle disposizioni di cui ai precedenti articoli; In particolare l'autorizzazione al traffico dati per la navigazione internet e per la posta elettronica è rilasciata dal Referente ICT;

2. L'ICT potrà installare sul telefono cellulare fornito dall'Azienda o sul quale sia utilizzata una scheda SIM fornita dall'Aziendaun'applicazione che garantisca la sicurezza dei dati contenuti all'interno del dispositivo (MDM).

Art. 16. Documentazioni addebiti.

1. I tabulati telefonici con l'indicazione del traffico effettuato per servizio saranno fatti pervenire con cadenza periodica all'utilizzatore e saranno comunque controllati a campione dall'ICT.

2. Per le chiamate di servizio l'Utente dovrà segnalare eventuali anomalie rilevate.

Art. 17. Limitazioni d'uso.

1. Il telefono mobile è un apparecchio per radiocomunicazioni che emette onde elettromagnetiche che in taluni luoghi e situazioni potrebbero interferire con le apparecchiature elettromedicali.

2. Allo scopo di evitare detto rischio gli operatori sono tenuti a seguire le eventuali indicazioni specifiche.

Art. 18. Verifica utenze assegnate.

1. Le utenze attualmente assegnate verranno sottoposte a verifica periodica di compatibilità con la normativa vigente mediante l'invio di un elenco utenze assegnate ai Referenti Interni che dovranno confermare o revocare le assegnazioni, restituendo firmato l'elenco appositamente trasmesso dall'ICT.

Art. 19. Cessazione della disponibilità dei servizi informatici aziendali.

1. Ai sensi del presente "Disciplinare", la disponibilità dei servizi informatici aziendali cesserà nei seguenti casi:

a) qualora non sussistesse più la condizione di dipendente o di collaboratore. Questo evento dovrà essere comunicato tempestivamente da parte del Direttore del Servizio Comune Gestione del Personale, in modo da poter eliminare dai SIA tutte le abilitazioni;
b) qualora non fosse confermata o venisse revocata l'autorizzazione all'uso fornita dal Referente interno.

Art. 20. Dismissione o cessione di supporti informatici e cartacei contenenti dati personali.

1. In caso di reimpiego, riciclaggio e dismissione, a qualsiasi titolo, di SIA e comunque, di apparecchiature elettriche ed elettroniche gli Utenti sono tenuti ad adottare una delle seguenti misure, anche chiedendo il supporto dell'ICT:

    a) cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l´utente abbia eliminato dei file da un´unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati, il tutto secondo un numero di ripetizioni del procedimento che tenga conto della delicatezza o dell'importanza delle informazioni di cui si vuole impedire l´indebita acquisizione
    b) formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità
    c) demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).
    d) procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali quali, a scelta dell'ICT, sistemi di punzonatura o deformazione meccanica, distruzione fisica o di disintegrazione o demagnetizzazione ad alta intensità.

Art. 21. Verifiche e controlli.

1. Le attività di verifica e controllo sono svolte dall'ICT esclusivamente per le seguenti finalità:

    a) motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware e software, etc.). Si rammenta che la preparazione di un nuovo

SIA comporta la possibilità dell'ICT di accedere alla casella di posta dell'utente e ai file temporaneamente salvati sul disco locale.;
b) tutela del sistema informatico e/o del patrimonio informativo aziendale;
c) controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.);
d) sicurezza del sistema informatico e verifica dell'efficacia delle misure di sicurezza adottate a protezione di dati, informazioni e infrastrutture;
e) prevenzione e riduzione, ove possibile, dei rischi connessi ad eventuali illeciti attraverso l'uso del Sistema Informativo aziendale;
f) applicazione delle procedure e dei regolamenti aziendali, adottati anche in osservanza di norme di legge.

2. Le attività di verifica e controllo sono svolte sugli strumenti e non sulle persone, e non sono mai svolte per finalità di controllo dell'attività lavorativa.

3. Le attività di verifica e controllo sopra descritte svolte dall'azienda possono essere di due tipi:

    a) di routine: eseguiti con periodicità sistematica dall'ICT attraverso l'uso di strumenti specificatamente predisposti ed appositamente parametrati, e hanno come scopo quello di consentire l'ordinaria gestione e manutenzione tecnica dei sistemi con la finalità di garantirne il corretto funzionamento o di applicare procedure e regolamenti aziendali;
    b) occasionali e puntali: sono quelli svolti occasionalmente a fronte di specifici eventi e circostanze atte, anche potenzialmente, a compromettere il funzionamento, la sicurezza e l'integrità del Sistema Informativo e del patrimonio aziendale. Tali controlli sono sempre condotti nel modo meno invasivo possibile, limitatamente alle sole aree del sistema interessate dagli eventi che generano la verifica, non prolungate nel tempo e limitate al periodo strettamente necessario ad assicurare funzionalità e sicurezza dei sistemi. I controlli di tipo occasionale e puntuale sono svolti dall'ICT su richiesta o autorizzazione della Direzione Aziendale o dei singoli Referenti, esclusivamente nei seguenti casi:

        1) per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
        2) nel caso in cui si verifichi un evento dannoso o una situazione di particolare gravità che richiede un intervento immediato a fronte della possibile compromissione dei sistemi.

4. In ogni caso, eventuali controlli occasionali e puntuali, saranno svolti nel rispetto delle modalità di seguito descritte:

    a) controllo preliminare dei dati (es. log) in forma anonima e aggregata riferiti all'intero sistema informatico e all'intera organizzazione lavorativa;
    b) se necessario invio di un avviso collettivo/generalizzato contenente la segnalazione di un rilevato incidente, utilizzo anomalo, di un abuso o di un comportamento non conforme al presente Disciplinare, accompagnato dall'avvertimento che, in caso di reiterazione, l'ICT potrà procedere ad una verifica anche a carico di singole e specifiche aree o del singolo SIA;
    c) nel caso in cui le anomalie o gli abusi rilevati persistano o generino problemi o incidenti successivi, l'ICT procede all'invio di un avviso

destinato solo ad un'area determinata o a un singolo utente, ed al conseguente controllo/verifica eventualmente anche a carico di singole e specifiche aree o delle singole utenze o SIA. I controlli sui singoli utenti saranno sempre svolti dall'ICT, alla presenza dell'Utente e, su richiesta dell'Utente medesimo, di un rappresentante dei lavoratori.