CENTRO SERVIZI
Benedetto Albertini
Via del Donatore di Sangue n° 4 - 37063 Isola della Scala (Verona)

ALLEGATO A) ALLA DELIBERAZIONE DEL C.D.A. N. 38 DEL 13.12.2021

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, POSTA ELETTRONICA E INTERNET

Sommario

INTRODUZIONE

In un mercato sempre più competitivo, dove i margini temporali d'azione si riducono in modo esponenziale, una delle chiavi dell'efficacia dei processi aziendali è rappresentata sicuramente dalle informazioni che tali processi ricevono, producono, processano e trasmettono.
I moderni sistemi informatici, con il loro prezioso carico informativo, si sono trasformati negli anni in uno dei principali asset sul quale costruire il successo del business e dal quale la sua durata nel tempo può dipendere.

La pronta **disponibilità** delle informazioni, la loro **accuratezza** e **integrità**, la loro **riservatezza** rivestono oggi un ruolo centrale nella tutela del patrimonio informativo.
Difendere questi aspetti significa porre delle solide basi per la continuità del business e per preservare l'immagine del Centro Servizi Benedetto Albertini (di seguito "**CSBALB**").

Con il presente documento, pertanto, s'intende uniformare la gestione e l'utilizzo degli strumenti informatici personali/collettivi in relazione alle attività svolte all'interno del CSBALB. Attraverso l'utilizzo delle risorse informatiche e telematiche del CSBALB, infatti, si deve evitare che comportamenti inconsapevoli possano generare problemi o minacce alla protezione dei dati personali, agli strumenti e a tutti i documenti aziendali rilevanti.
Tutte le tecnologie informatiche ed elettroniche a disposizione, che vengono fornite e configurate in modo sicuro, devono essere utilizzate ispirandosi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro.
Le prescrizioni e le indicazioni che seguono si aggiungono ed integrano le altre policy aziendali e le specifiche istruzioni già fornite a tutti gli "Autorizzati/incaricati al trattamento" ed al personale delegato di specifici compiti (Delegati Privacy).

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente Regolamento, è possibile rivolgersi al Responsabile della Unità Operativa Sistemi Informativi (UOSI), al Referente aziendale privacy e al Responsabile della Protezione dei Dati (DPO).

A. SCOPO E CAMPO DI APPLICAZIONE

Con il presente Regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche che il CSBALB mette a disposizione del personale dipendente e non dipendente (di seguito "**Utenti**") per l'esecuzione delle funzioni di competenza.

Sono altresì disciplinate le modalità con le quali il CSBALB può accertare e inibire le condotte illecite degli utilizzatori di Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server, hard disk).

Sono tenuti all'osservanza delle presenti disposizioni tutti gli Utenti interni ed esterni che sono autorizzati ad accedere al Sistema Informatico Aziendale e ad utilizzare le strumentazioni elettroniche fornite per l'esecuzione delle mansioni lavorative.

Per **Utenti interni** si intendono le persone fisiche che, sulla base di rapporti contrattuali o convenzionali autorizzati dalla Direzione del CSBALB, possono utilizzare all'interno del "dominio aziendale" gli strumenti informatici del CSBALB.

Per **Utenti esterni** si intendono le persone fisiche, le Aziende private e Pubbliche e le ditte fornitrici che, sulla base di rapporti contrattuali o convenzionali autorizzati dalla Direzione del CSBALB, accedono dall'esterno del "dominio aziendale" ad alcune componenti del Sistema Informatico Aziendale.

Tali soggetti possono essere individuati come "Designati di specifici compiti e funzioni (Delegati Privacy)" o quali "Autorizzati al trattamento" dei dati personali ai sensi del Regolamento UE 2016/679, mentre i soggetti "esterni" al CSBALB, nei casi relativi a collaborazione di persone fisiche o giuridiche (convenzioni, consulenze, tirocini, appalti, ecc.), possono operare in qualità di responsabili del trattamento; d'ora in avanti sono denominati tutti anche con il termine "Personale".

All'interno del documento non sempre vengono fornite indicazioni puntuali in quanto, dato l'ambito in continuo sviluppo, risulterebbe difficile se non impossibile contemplare ogni tipologia di dispositivo informatico e di informazione di interesse aziendale. Risulta per tale ragione un fattore chiave comprendere la logica alla base e le finalità del presente documento per poter seguire in modo efficace le indicazioni fornite.

Quanto segue è redatto nel pieno rispetto delle leggi regolatrici dei rapporti di lavoro e del Provvedimento a carattere generale emesso Garante per la protezione dei dati personali il 1° marzo 2007 (relativo all'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro) ed è pertanto indispensabile la sua conoscenza da parte di tutti i dipendenti e collaboratori del CSBALB.

Una corretta esecuzione del presente Regolamento presuppone il pieno assolvimento da parte del CSBALB degli obblighi contenuti nella Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativa alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» e s.m.i., nonché di eventuali provvedimenti in materia emanati da organismi operanti nel medesimo settore.

B. RIFERIMENTI NORMATIVI E DOCUMENTALI

NORMATIVA EUROPEA

- **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 personali").

NORMATIVA ITALIANA

- **Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni** ("Codice in materia di protezione dei dati personali").
- **Legge 20 maggio 1970, n. 300** , norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento (detta anche "statuto dei lavoratori").
- **Decreto Legislativo 8 giugno 2001, n. 231**, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Azienda e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.

CODICE CIVILE

- Art. 2049: Responsabilità indiretta dell'imprenditore;
- Art. 2086: Direzione e gerarchia nell'impresa;
- Art. 2087: Tutela dell'integrità fisica e della personalità morale dei dipendenti, da parte dell'imprenditore;
- Art. 2104: Diligenza del dipendente nel rispetto delle disposizioni impartite dall'imprenditore.

PROVVEDIMENTI AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- **Linee Guida del Garante Privacy su Posta Elettronica e Internet** (Deliberazione n. 13 del 1° marzo 2007 – G.U. n. 58 del 10 marzo 2007);
- **Provvedimento del Garante Privacy del 27 novembre 2008** e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema";

AGENZIA PER L'ITALIA DIGITALE - AGID

- Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativo a «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

C. DEFINIZIONI

Dati

Ai sensi del Regolamento UE 2016/679, i dati possono essere classificati come segue:

- **Personali**: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Sono dati personali: nome e cognome, indirizzo, codice fiscale, foto, l'indirizzo IP o qualsiasi altra ripresa audiovisiva. La persona difatti può essere identificata anche attraverso altre notizie che non siano direttamente identificative (ad esempio, associando la registrazione della voce di una persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione).
- **Categorie particolari di dati**: dati personali che, per la propria delicatezza, richiedono particolari cautele; essi sono quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o all'orientamento sessuale della persona.
- **Dati relativi a condanne penali e reati**: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (quali dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.)

Trattamento dei dati

Per **trattamento dei dati** si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

Operazioni sui dati

Pertanto, le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

i. ***Il reperimento delle informazioni***

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi o un sito web.

ii. ***Il trattamento "interno" delle informazioni*.**

Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili.

Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, eccetera;

- l'elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, l'estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

iii. ***L'uso delle informazioni nei rapporti con l'esterno***

Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della riservatezza altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni. L'utilizzo può essere:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni;
- indiretto, ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive dei diritti e delle libertà degli interessati, sono quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:

- la **comunicazione**, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- la **diffusione**, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Per lo svolgimento delle quotidiane attività lavorative, il CSBALB, che è titolare del trattamento, necessita dell'utilizzo di apparecchiature informatiche per l'espletamento di molteplici compiti, nell'ambito di diversi ruoli e posizioni organizzative.

L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti - anche inconsapevolmente non leciti - possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati), sia sul piano giuridico (che possono determinare l'insorgere di responsabilità sia penali sia civili a carico, contestualmente, del titolare e del lavoratore coinvolto).

D. NORME COMPORTAMENTALI

Norme tecniche

Tutto il Personale che utilizza strumenti elettronici è tenuto a prendere visione e attenersi a quanto previsto nel presente Regolamento.

Il Personale che tratta dati personali è tenuto al rispetto di tutte le apparecchiature messe a disposizione dal CSBALB, provvedendo alla buona conservazione delle stesse, avendo cura al termine dell'orario di lavoro di lasciare la propria postazione di lavoro ordinata, efficiente e con le apparecchiature spente salvo indicazioni contrarie da parte dei responsabili delle strutture e della UOSI.

Al momento di lasciare i locali e gli uffici, il Personale dovrà, altresì, accertarsi della chiusura di finestre dei locali da loro occupati.

I personal computer ed i dispositivi mobili aziendali utilizzati dal Personale sono strumenti di lavoro. Ogni utilizzo improprio può causare disservizi, costi impropri di manutenzione e, soprattutto, minacce alla sicurezza ed alla protezione dei dati personali nonchè alle informazioni costituenti patrimonio aziendale.

Nei personal computer forniti è sconsigliato l'inserimento di supporti magnetici o ottici (CD-ROM, DVD–ROM, Pen Drive, etc.), se non espressamente autorizzati o verificati dal Responsabile della UOSI o suo delegato.

Gli Utenti non devono modificare la configurazione del proprio personal computer; in caso di mal funzionamento dovranno richiedere l'intervento dei tecnici preposti. Si fa inoltre assoluto divieto di installare sulle apparecchiature software non autorizzati. Si ricorda che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente.

E' assolutamente vietato modificare i dati contenuti nei programmi gestionali salvo quelli esplicitamente autorizzati ed è altresì vietato effettuare modifiche, attraverso gli strumenti di sviluppo, di qualsivoglia componente del programma stesso.

Tutta la documentazione prodotta dal Personale autorizzato al trattamento dovrà essere elaborata con gli strumenti messi a disposizione dal CSBALB e dovrà essere inserita nelle cartelle autorizzate; periodicamente verrà effettuato un controllo dei dischi fissi al fine di verificarne l'efficienza, provvedendo all'eliminazione dei file superflui. È fatto divieto di salvare file e/o cartelle in posizioni non autorizzate.

Non è consentita la memorizzazione di documenti informatici contenenti dati personali su dischi locali del pc.

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Poiché i malware, ovvero un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al sistema su cui viene eseguito (rientrano in questa categoria virus, worm, spyware e altri programmi dannosi), costituiscono una delle minacce più frequenti alla sicurezza, è necessario che il Personale autorizzato al trattamento si attenga alle seguenti norme:

- il sistema informatico presenta software di protezione che vengono aggiornati automaticamente. Si raccomanda, pertanto, di verificare periodicamente l'effettivo funzionamento del sistema e di non disattivarli in nessuna occasione;
- è necessario evitare il materiale che potrebbe contenere virus o altri software dannosi;
- non scaricare mai file da mittenti sconosciuti o sospetti e, quando necessario, effettuare sempre un controllo prima di acquisire o aprire qualunque programma o documento acquisito via posta elettronica (in caso di dubbio contattare la UOSI).

Sistemi informativi

Salva schermo protetto con password

All'interno della rete i dispositivi sono protetti da una impostazione del sistema operativo che dopo un breve periodo di inattività dell'elaboratore lo blocca attivando uno screen saver protetto con password robusta (d'ora in avanti semplicemente *password*). Ciononostante, il Personale è tenuto a bloccare il proprio computer (fisso o laptop) nelle pause previste o nel momento in cui debba allontanarsi da esso per più di qualche minuto (ad esempio attivando il blocca schermo, digitando Ctrl+Alt+Canc, Blocca computer).

Unità disco di rete

Il CSBALB dispone dei così detti "Dischi di Rete". Si tratta di spazi di memorizzazione dedicati ai file degli Utenti e che vengono protetti con sistemi avanzati di back up. Questa protezione garantisce la disponibilità del dato in caso di perdita dei dispositivi di memorizzazione. I file che vengono prodotti in locale devono essere salvati anche nel disco di rete e una volta che non sussistano più ragioni di convenienza i file locali devono essere eliminati a favore della sola conservazione sul disco di rete. Le cartelle nei dischi di rete possono essere create per area e per un singolo dipendente. Vedere anche il punto successivo per la cartella personale nei dischi di rete.

Cartella personale

Nei dischi di rete è presente una cartella (dedicata o nominativa) per il salvataggio dei propri dati. In tale cartella devono essere salvati tutti i file del personale dipendente, anche se memorizzati inizialmente in locale su personal computer e laptop.
In caso di furto o smarrimento dei dispositivi portatili, infatti, la copia "in rete" dei file garantirà la disponibilità delle informazioni aziendali. Come già evidenziato in precedenza si invita il Personale a mantenere le sole informazioni necessarie sul disco locale, utilizzando principalmente il disco di rete al fine di garantirne la disponibilità e la riservatezza in caso di eventi dannosi.

Cartelle locali

Le cartelle create localmente nei personal computer e laptop sono da intendersi come temporanee e l'eventuale contenuto deve esistere in copia di sicurezza anche nei dischi di rete.
Il loro uso tipico è quello di permettere al personale dipendente di lavorare su file aziendali anche quando si trova al di fuori della rete aziendale.
Non è ammessa l'archiviazione di file con dati personali.

Supporti di memorizzazione

Occorre salvare sempre le informazioni confidenziali sul vostro server di rete e non all'interno dello strumento elettronico, non salvare informazioni in particolare se contengono categorie particolari

di dati personali su supporti rimovibili e, nel caso vi sia la necessità di consegnare a terzi supporti rimovibili per trasferire dati accertarsi della relativa criptazione, assicurarsi che sulla chiave di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare la chiave a terzi, che potrebbero copiare le informazioni personali memorizzate;
Eliminare sempre documenti, dischetti o altri supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili e accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutili messaggi di posta elettronica.

Utilizzo di Personal Computer

I Personal Computer (PC) vengono assegnati individualmente a singoli Utenti interni, che rispondono del loro utilizzo e devono custodirli con diligenza sia durante gli spostamenti, sia durante l'utilizzo intra ed extra aziendale.
Se l'utilizzo del PC è condiviso da più utenti, il PC è assegnato al Direttore dell'UOC di competenza.
Occorre prestare attenzione a non lasciare mai incustodito lo strumento in ufficio o in viaggio in caso di PC portatili (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici).
Durante le eventuali missioni di lavoro, portare il PC portatile come bagaglio a mano, evitando di trasportare in borsa i codici identificativi e le parole chiave di sicurezza, nonché i supporti di memorizzazione con le copie di back-up.
È vietato lasciare incustodito sull'autovettura lo strumento aziendale, anche se per soste brevi, indipendentemente dalla visibilità o meno dello strumento dall'esterno.

Software

Sugli strumenti in dotazione possono essere utilizzati solamente software forniti dal CSBALB; pertanto non si possono acquistare e installare software e applicazioni senza una specifica verifica e autorizzazione da parte della UOSI Sistemi Informativi.
Non installare da soli i software sul PC in dotazione, se non previa autorizzazione da parte della UOSI e non creare e non utilizzare software senza licenza d'uso (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 sulle nuove norme di tutela del diritto d'autore). E' vietata ogni forma di copia del software; tali comportamenti includono: l'inoltro di mail o altri documenti riprodotti tramite foto, video o copia cartacea verso l'esterno, se non per attività lavorative, e vietano altresì il re-inoltro ad altri account che non siano quelli aziendali

Accesso ed uso dei sistemi e password

Le unità disco (locali o di rete) sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia connesso all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. È vietata, anche, la conservazione e l'archiviazione dei dati in locale sui singoli PC, salvo alcune specifiche eccezioni legate a esigenze produttive.

Il Personale si connette alla rete del CSBALB tramite autenticazione univoca personale. Il Personale è tenuto a non rivelare ad alcuno le credenziali di autenticazione (UserID e password) ad alcuno, colleghi, superiori amministratori di sistema inclusi, dovendo avere la massima diligenza nella custodia delle stesse e preservandone la segretezza anche durante il momento della digitazione. La connettività attraverso reti geografiche protette (VPN – Virtual Private Network) è permessa previa autorizzazione scritta da parte del Direttore.

Qualora il Personale prenda coscienza che taluno possa aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente provvedere cambiarla. Qualora sia richiesto di riferire in qualunque forma la password (telefonicamente, via e-mail, ect.) il Personale è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto al Responsabile della UOSI.

Non debbono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.

È vietato comunicare, scambiare o condividere password tra più utenti (neanche se appartenenti al medesimo team di lavoro) o divulgare password personali a terzi (anche se colleghi o amministratori di sistema); la condotta non conforme a questa prescrizione può comportare sanzioni disciplinari.

La password scelta non deve avere relazione con la propria vita privata e aziendale e deve essere di almeno otto caratteri.

È vietato riutilizzare le proprie password lavorative (es. di accesso al pc, alla posta o ai vari applicativi) per la registrazione in altri siti web.

Il Personale ha l'obbligo di cambiare la password di accesso agli strumenti informatici almeno ogni 90 giorni. Solo in casi eccezionali la password potrà essere resettata a cura del personale della UOSI.

Occorre conservare le password con diligenza per impedire che soggetti terzi ne vengano a conoscenza, segnalandone sollecitamente al personale della UOSI l'eventuale smarrimento, sottrazione o diffusione.

In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo sia informatico.

I requisiti minimi di complessità delle password sono:

- redazione con caratteri maiuscoli e/o minuscoli;
- utilizzo di simboli, numeri, punteggiatura e lettere;
- numericamente devono essere password di almeno 8 caratteri;
- non deve trattarsi di password basate su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.

La password deve essere mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia.

Posta Elettronica

Email Aziendale (email standard)

Il servizio di Posta elettronica viene fornito, dal CSBALB, in funzione della comunicazione, della amministrazione e delle altre attività strumentali correlate ai fini istituzionali. Il servizio è subordinato all'osservanza integrale delle condizioni contenute nel Regolamento. L'utilizzo del servizio da parte dell'Utente costituisce implicita accettazione delle citate condizioni.

Sono attivati indirizzi di posta elettronica per le strutture aziendali, condivisi dagli operatori assegnati a ciascuna di esse con l'estensione NOMESERVIZIO@cralbertini.it (es. protocollo@cralbertini.it).

Al singolo Utente può essere assegnato un indirizzo e-mail aziendale personale del tipo: nome.cognome@cralbertini.it, ovvero riferito al servizio, con eccezioni previste per i casi di omonimia.

Questi alla data attuale i servizi comuni previsti dal CSBALB:

protocollo@
infermieri@
educatori@
fisioterapisti@
logopedista@
psicologa@

eventuali altri indirizzi comuni potranno venire creati secondo le esigenze operative future.
La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del Personale al solo fine dello svolgimento delle proprie mansioni lavorative; non è consentito l'utilizzo per motivi diversi da quelli inerenti all'espletamento degli adempimenti lavorativi ed è vietato l'utilizzo dell'indirizzo di posta elettronica per fini privati.

L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della sua password e a segnalare qualunque situazione che possa inficiarla. L'Utente sarà responsabile dell'attività espletata tramite il suo account.

L'Utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:

- comunicazioni commerciali private;
- materiale in violazione della Legge n. 269 del 1998;
- materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
- materiale che violi le normative sulla protezione dei dati personali;
- contenuti o materiali che violino i diritti di proprietà di terzi;
- altri contenuti illegali.

L'elenco riportato è da intendersi meramente esemplificativo e non esaustivo. In nessun caso l'Utente potrà utilizzare la posta elettronica aziendale per diffondere codici dannosi per i computer quali virus e simili.

Si deve evitare di rispondere alle "catene di Sant'Antonio" degli utenti di internet o ai messaggi di solidarietà che richiedono di inviare un'e-mail a un certo indirizzo o a un certo numero di utenti, poiché possono essere veicoli di diffusione di virus informatici, ovvero sistemi per la raccolta di indirizzi di posta elettronica, per l'invio di comunicazioni commerciali non desiderate o di posta "spazzatura", nonché si deve evitare di rispondere a messaggi promozionali o di spamming.

È fatto divieto di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.

Si rende noto che per motivi organizzativi e funzionali, vengono archiviati tutti i messaggi di posta elettronica (anche nelle copie di back up), in uscita ed in entrata dalle caselle di posta elettronica del CSBALB. Conseguentemente, stante la natura di strumento di comunicazione aziendale del sistema di posta elettronica, il Personale è consapevole che sullo stesso non potrà essere garantita la riservatezza del messaggio e dei documenti inviati e ricevuti; pertanto, sarà impegno del Personale evitare l'utilizzo delle caselle di posta elettronica per comunicazioni di carattere personale o che esulino dal contesto aziendale a cui sono preposte.

Nei messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominative) verrà accluso il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente".*

Posta Elettronica Certificata (PEC)

La Posta Elettronica Certificata (detta anche PEC) è un sistema di comunicazione simile alla posta elettronica standard ma tra indirizzi mail certificati, a cui si aggiungono caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere valore legale ai messaggi trasmessi.

Il **valore legale** è assicurato dai gestori di posta PEC del mittente e del destinatario che certificano:

- data e ora dell'invio del messaggio dal parte del mittente;
- data e ora dell'avvenuta consegna del messaggio al destinatario;
- integrità del messaggio (e eventuali allegati) nella trasmissione da mittente a destinatario.

I gestori di posta assicurano anche notifica al mittente e al destinatario di eventuali problemi occorsi durante la trasmissione. La PEC trasferisce sul digitale il concetto di "**Raccomandata con Ricevuta di Ritorno**". L'utilizzo della posta elettronica rispetto alla posta tradizionale garantisce la consegna in tempo reale.

Valore legale: a differenza della tradizionale posta elettronica, alla PEC è riconosciuto pieno valore legale e le ricevute possono essere usate come prove dell'invio, della ricezione ed anche del contenuto del messaggio inviato.

La comunicazione ha valore legale solo se inviata da PEC e ricevuta da PEC. L'estensione PEC: cralbertini@pec.it, accetta esclusivamente documenti provenienti da caselle di PEC, al fine di garantire gli utenti contrastando il fenomeno dello spamming e gli usi impropri.

Liste di distribuzione

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list), personali o centralizzate. L'Utente può avvalersi di liste di distribuzione personali, per le proprie necessità funzionali, a fronte di esigenze tecniche e/o gestionali. Una lista generale di distribuzione, centralizzata e comprendente tutti gli utenti, è gestita dal Responsabile della UOSI.

Oltre alla lista generale di distribuzione, sono possibili altre liste centralizzate (o gruppi) utili a soddisfare le esigenze di categorie omogenee di utenti (es. Personale Sanitario, Dirigenza Medica ecc..); l'attivazione di questi gruppi è a cura del Responsabile della UOSI che valuterà, di volta in volta, le specifiche richieste.

Si fa presente che l'utilizzo di tali liste permette l'accesso ai messaggi da parte di tutti gli iscritti alla lista di distribuzione collegata a quell'indirizzo. Per tale motivo, sugli account sopra indicati non può essere garantita la riservatezza delle comunicazioni.

Le informazioni aziendali riservate, inoltre, sono segrete e oggetto di specifica tutela e, come tali, sono sottoposte a misure di sicurezza adeguate a mantenerle segrete.

A tal fine, pertanto, si ricorda che:

- non è consentito l'utilizzo degli indirizzi di posta elettronica del CSBALB per la partecipazione a dibattiti, Forum, newsletter o mailing list, non attinenti l'attività lavorativa;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e

appartenenza sindacale e/o politica, handicap o stato di salute o che costituiscano comunque condotta illecita;

- è vietato l'inoltro dei messaggi ricevuti sull'account di posta aziendale ad altro indirizzo e-mail personale del personale dipendente;
- è severamente vietato inviare messaggi, con allegati file con contenuti inerenti alle attività del CSBALB a destinatari che non sono in relazione con la stessa e/o non sono autorizzati a riceverli, salvo espressa autorizzazione scritta del titolare.

Utilizzo e controlli

È severamente vietato inviare messaggi attraverso lo strumento dell'e-mail semplice con allegati file (o nel corpo del testo) contenenti categorie particolari di dati o dati relati a condanne penali o reati. Tali dati possono essere trasmessi previa idonea protezione atta ad impedire la relativa lettura da parte di soggetti non autorizzati.
In conformità delle disposizioni di legge e nel pieno rispetto del principio di non eccedenza, il CSBALB si riserva la facoltà di effettuare controlli circa le modalità e le finalità di utilizzo della posta elettronica, soprattutto al fine di verificare la funzionalità e la sicurezza del sistema informatico. Ciò avverrà avvalendosi della facoltà di effettuare i c.d. "controlli difensivi" (attraverso soggetti all'uopo preposti), che saranno effettuati saltuariamente e/o a campione e solo in caso di stretta necessità, sull'intera area del traffico dati della posta elettronica del CSBALB ed esclusivamente per finalità di difesa e tutela del patrimonio e della sicurezza della struttura titolare del trattamento. A tal fine e per esigenze tecniche o di manutenzione, gli amministratori di sistema possono trovarsi ad avere accesso ai contenuti delle e-mail aziendali (in ogni caso non saranno effettuate verifiche massive, prolungate e/o indiscriminate).

Il CSBALB fa presente al Personale che il servizio di posta elettronica fornito mediante l'attribuzione di un account aziendale è uno "strumento di lavoro", al pari degli altri servizi della rete aziendale, fra cui anche il collegamento a determinati siti internet. Costituiscono parte integrante di questi strumenti, anche i sistemi e le misure – in uso presso il CSBALB - che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, che conserva i soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una durata non superiore a sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

Salvo quanto sotto indicato, in nessun caso verrà effettuato l'accesso diretto alle caselle di posta elettronica in uso al Personale, se non in seguito a gravi e comprovati motivi che possano rilevare il compimento di reati o condotte illecite oppure su segnalazione dell'Autorità Giudiziaria nell'ambito di indagini svolte per la repressione, accertamento e prevenzione di reati. In caso di un eventuale accesso all'account di posta elettronica concesso in uso al Personale, i dati dei terzi saranno tutelati e l'identità degli interlocutori dell'Utente non sarà rivelata (nemmeno in eventuali sedi giurisdizionali).

Il Personale, eventualmente, potrà richiedere la possibilità di utilizzare un account di posta elettronica privata, per le comunicazioni di carattere personale; in ogni caso, CSBALB si riserva il diritto di concedere o meno tale privilegio a seconda della effettiva necessità.

Nel caso di assenza programmata e al fine di non interrompere, né rallentare i processi produttivi e/o lavorativi, l'Utente ha la facoltà di predisporre la funzionalità che permette l'invio di un messaggio automatico di risposta che segnali altro nominativo e relativo indirizzo di posta elettronica di un collega da contattare nel caso di urgenze; il delegato potrà in questo modo ricevere i messaggi di posta elettronica del dipendente assente e a lui indirizzati.

Si dispone, inoltre, che nel messaggio automatico di risposta siano evidenziati l'inizio e la fine del periodo di assenza del dipendente, secondo il seguente modello: *"Sarò assente dal___al___Per urgenze, contattare il sig. ____al n. ____o all'indirizzo e-mail ____ "*.

Un Utente interno può nominare una persona di fiducia che, in caso di una sua assenza, può avere accesso alla sua casella di posta al fine di garantire la continuità dell'attività lavorativa. In mancanza di questa nomina e in caso di assenza improvvisa o prolungata del dipendente, se è necessario conoscere il contenuto di messaggi di posta elettronica inviati all'indirizzo aziendale o nel caso di motivi di manutenzione o urgenza, un soggetto delegato dal CSBALB (Direttore della propria UOC) sarà legittimato a visionare i messaggi di posta elettronica del lavoratore assente previa comunicazione all'Utente.

Il personale dipendente è tenuto ad accedere alla casella e-mail assegnata con frequenza almeno giornaliera e a usare tale strumento per qualsiasi comunicazione interpersonale nell'ambito delle finalità lavorative. Le informazioni trasmesse, molto spesso, possono o devono essere condivise per cui deve essere salvaguardata l'integrità e la confidenzialità dei messaggi e dei contenuti.

È fatto divieto in ogni caso di divulgare a soggetti non autorizzati le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal dovere di segretezza a cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.

Al termine della collaborazione lavorativa con il CSBALB per qualsiasi motivo (es. pensionamento, licenziamento, trasferimento presso altro datore di lavoro etc.), l'eventuale account nominativo di posta elettronica aziendale dell'Utente (di proprietà del CSBALB) sarà disattivato alla data di cessazione del rapporto di lavoro e di collaborazione con CSBALB. Alla disattivazione dell'account seguirà la cancellazione dell'indirizzo di posta elettronica aziendale. Le emails saranno conservate solo ai fini di tutela dei diritti in sede giudiziaria, nei limiti di cui all'art. 160-bis, c. 1 del D.Lgs. 196/2003.

<u>Navigazione in Internet</u>

La finalità dell'accesso e della navigazione su Internet è il reperimento di informazioni e di documentazione utili al CSBALB; l'utilizzo dei servizi di rete per scopi non inerenti ai fini aziendali è consentito limitatamente alla pausa lavorativa e nel rispetto delle leggi e dei regolamenti vigenti.

Non saranno normalmente esercitati controlli in relazione alla navigazione effettuata in tale lasso temporale, salvo in caso di segnalazione o richieste da parte di Autorità competenti preposte alla prevenzione di illeciti informatici.

Durante il resto della giornata lavorativa è fatto divieto al Personale di navigare in siti non attinenti con l'attività lavorativa, in quanto l'utilizzo al collegamento ad Internet deve essere funzionale all'attività espletata in favore del CSBALB. Una violazione di tale prescrizione - e qualora vengano perpetrati eventuali illeciti nella navigazione in internet - potrebbe comportare sanzioni disciplinari a carico del contravventore attraverso le modalità e le procedure in seguito indicate al paragrafo "Controlli indiretti".

Al fine di garantire la sicurezza dei propri dati, nonché di favorire un utilizzo corretto dello strumento Internet, CSBALB potrebbe adottare alcuni accorgimenti tecnici per prevenire illeciti da parte del Personale (è facoltà del CSBALB, infatti, implementare delle misure preventive e delle "black list" di siti Internet aventi l'obiettivo di impedirne la visione in quanto non ritenuti d'interesse aziendale). Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, il CSBALB adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure indicate al paragrafo "Controlli indiretti".

Il CSBALB, al fine di prevenire determinate operazioni non consentite, ha implementato dei sistemi di filtro della navigazione che puntano a mitigare i rischi sopra esposti; ciononostante la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza dell'Utente. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, Il CSBALB adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure di seguito specificate:

- al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i PC aziendali hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'Utente, garantendo in tal modo il suo anonimato. L'accesso a questi dati è effettuato dal Responsabile della UOSI e da persone afferente tale struttura appositamente autorizzato, nonché eventualmente da personale tecnico esterno autorizzato dalla Direzione Generale;
- il CSBALB ha attivato tali sistemi secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali (Provvedimento del 1° marzo 2007), effettuando monitoraggio generalizzato ed anonimo dei log di connessione. Pertanto, in seguito al rilevamento di anomalie nel sistema dei dati, per motivi di manutenzione o in caso di comportamenti anomali individuati in una determinata area o a seguito di controlli a campione saltuari, il CSBALB potrà attivare meccanismi di monitoraggio delle attività di rete (file di log) e di controllo del traffico internet o del traffico della posta elettronica o dei file di back up per fini organizzativi o di manutenzione, per verifiche sulla funzionalità del sistema o di controllo della sicurezza dell'impianto. Gli archivi di log risultanti da questo monitoraggio, effettuati in determinate aree del CSBALB e allo stesso tempo sufficientemente grandi da garantire la riservatezza dei lavoratori, contengono traccia di ogni operazione di collegamento effettuata dall'interno del CSBALB verso Internet.

In caso di accertata violazione definita tramite alert, il Responsabile della UOSI provvederà prontamente a segnalare all'interessato l'attività illecita riscontrata.
Nel rispetto al principio di finalità, pertinenza e non eccedenza, tali log vengono tenuti negli archivi del CSBALB per 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Azienda e può accedere a tali informazioni solo il personale della UOSI. L'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

Al fine di evitare il grave rischio di importazione di virus informatici e di pregiudizio alla stabilità delle applicazioni dell'elaboratore, non è consentita l'autonoma installazione di programmi provenienti dall'esterno. Analogamente, non è possibile effettuare il download di file o di software aventi particolari caratteristiche dimensionali, tali da ridurre l'efficienza del sistema. Qualora, a seguito di controlli effettuati saltuariamente e a campione sul PC in uso all'utilizzatore, risultino presenti file o software non espressamente autorizzati, saranno posti in essere richiami disciplinari, motivati dal fatto che qualsiasi file o programma estraneo a quelli contenuti e autorizzati può cagionare incompatibilità con i programmi forniti e già in uso per lo svolgimento dell'attività lavorativa e/o costituire una minaccia per la sicurezza informatica. Il titolare, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi dell'art. 171-bis della L. 633/1941 (Legge sul diritto d'autore).

Non è permessa la partecipazione, per motivi non lavorativi, a Forum, l'utilizzo di chat line, di bacheche elettroniche, mailing list o altri mezzi di comunicazione telematica non attinenti con l'attività lavorativa, attuate mediante il pc affidato in uso.

Rete Dati

È vietato collegare alla rete dati aziendale strumenti elettronici che non siano stati autorizzati dal Responsabile della UOSI. Il computer in dotazione non deve possedere o disporre di altri collegamenti esterni diretti; è vietato installare mezzi di comunicazione propri (come per esempio il modem analogico).

Utilizzare esclusivamente le installazioni messe a disposizione da CSBALB, ovvero quelle che siano oggetto di specifica autorizzazione. Non usare mai il proprio nome utente e password per accedere a sistemi esterni.

Ricordarsi che CSBALB può monitorare il lavoro svolto e le connessioni, potendo verificare per motivi di sicurezza quali siti siano stati visitati e quali operazioni di trattamento sono svolte con i dati personali, di cui è titolare il CSBALB.

Non inviare informazioni confidenziali tramite internet o altre reti di comunicazione elettronica senza aver preso le dovute precauzioni e adottato le misure di sicurezza idonee a ridurre i rischi di accesso abusivo dei dati trasmessi.

Utilizzo del fax, telefono, cellulare, fotocopiatrici e stampanti

In generale, è opportuno non fornire indicazioni relative allo stato di salute degli utenti via telefono, se non si è certi dell'identità dell'interlocutore che sta chiamando; occorre verificare comunque che l'interessato abbia autorizzato la comunicazione dei propri dati a terzi.

In alcuni casi, specie per chiamate di natura istituzionale (da altre strutture di servizio oppure da strutture ospedaliere, autorità giudiziaria, soggetti pubblici), si consiglia di farsi lasciare dal chiamante il proprio nominativo e il numero di telefono; si provvederà a ricontattare l'ente chiamante, chiedendo della persona che ha lasciato il proprio nominativo, previa verifica dell'indispensabilità dei dati richiesti rispetto alla finalità dell'utilizzo dichiarato e della previsione normativa o dell'autorizzazione dell'interessato alla comunicazione dei propri dati.

Non deve essere usato il Fax per le comunicazioni tra il CSBALB e altri Enti Pubblici poiché l'articolo 14 "*Misure per favorire la diffusione del domicilio digitale*", del c.d. Decreto del Fare (in seguito alle modificazioni apportate dalla legge di conversione n. 98 del 9 agosto 2013) ha stabilito che ai fini della verifica della provenienza delle comunicazioni è in ogni caso esclusa la trasmissione di documenti a mezzo fax. In particolare, è vietato l'uso del fax nelle trasmissioni di documenti con altre Pubbliche Amministrazioni ai sensi dell'art. 47 del Codice dell'Amministrazione Digitale. Non deve parimenti essere usato il fax per le comunicazioni tra il CSBALB e gli enti privati o i cittadini, non costituendo obbligo nel nostro ordinamento ma solo facoltà, in tal modo favorendo un migliore andamento amministrativo e organizzativo del CSBALB medesima.

Il telefono, gli eventuali cellulari aziendali e le fotocopiatrici devono essere utilizzati per scopi puramente lavorativi.

Non è consentito rivelare numeri telefonici interni o informazioni sul CSBALB a persone non preventivamente identificate, nonché autorizzate a conoscerle, ed è fatto divieto di lasciare documenti incustoditi presso i locali delle fotocopiatrici. Ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari che potranno variare a seconda della gravità.

La stampa di documentazione contenente dati personali deve avvenire ad opera di personale autorizzato a trattare tali dati; inoltre, occorre ritirare tempestivamente la documentazione dalla stampante utilizzata (il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nella disponibilità dell'autorizzato ed essere utilizzati nell'ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti).

I fogli contenenti dati personali non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da renderli non intelligibili a terzi usando eventualmente un adeguato dispositivo distruggi documenti.

Segreto Professionale e informazioni riservate

Nella valutazione delle informazioni, il Personale si impegna a osservare ogni cautela perché le stesse rimangano riservate, essendo inteso che, in caso di divulgazione non autorizzata, sarà a suo carico l'onere di provare di avere adottato tali misure.

E' vietato in particolare comunicare e/o divulgare notizie di qualsiasi interessato di cui si venga a conoscenza nell'ambito della propria attività lavorativa, soprattutto in considerazione delle attività di cura e salute del CSBALB.

Il Personale non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in tutto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Tali comportamenti includono: l'inoltro di mail o altri documenti riprodotti tramite foto, video o copia cartacea verso l'esterno, se non per attività lavorative e vietano altresì il re-inoltro ad altri account che non siano quelli aziendali.

Gli obblighi del dipendente, descritti in questo documento, non termineranno all'atto di cessazione del rapporto di lavoro.

Misure organizzative e di sicurezza in ambito privacy

Ogni computer deve essere protetto da idonei strumenti per il rischio di attività di virus informatici; lo strumento di protezione (di norma software antivirus) deve essere abilitato ed è vietato disattivarlo; la posta elettronica viene filtrata in ingresso da un apposito prodotto antivirus che pulisce gli eventuali allegati contenenti virus. Evitare comunque di aprire messaggi provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente. In caso di dubbio contattare prontamente Responsabile della UOSI.

Nel caso di utilizzo di supporti di memorizzazione esterni fermo restando quanto previsto nel presente Regolamento in merito alla possibilità di utilizzo di detti supporti, controllare sempre che i file memorizzati non siano infettati da virus attraverso la scansione del supporto.

Tutto il personale dipendente che tratta dati ed è stato autorizzato al trattamento è tenuto al rispetto dei principi e delle misure organizzative e di sicurezza di cui alla normativa in materia di protezione dei dati personali e, in particolare, deve:

- trattare i dati personali secondo i principi indicati dalla legge, in modo lecito, corretto e trasparente; ciò vuol dire che deve verificare:
  - se il trattamento sia consentito da una norma di legge o di regolamento (es. in materia di sicurezza sul lavoro o normative fiscali) o,
  - se il soggetto i cui dati afferiscono (Interessato) abbia ricevuto idonea informativa e/o abbia eventualmente rilasciato il consenso (ove necessario) ovvero sussista altra base giuridica per il trattamento;

- controllare la pertinenza e non eccedenza dei dati raccolti e trattati rispetto alle finalità perseguita, evitando di accogliere dati inutili rispetto al raggiungimento della stessa attuando il "principio di minimizzazione" nel trattamento);
- controllare l'esattezza dei dati ed eventualmente, qualora si renda necessario, provvedere al loro aggiornamento;
- conservare i dati in una forma che consenta l'identificazione dell'Interessato per un periodo non superiore a quello necessario agli scopi della raccolta e mettere in atto procedure tali da realizzare la cancellazione degli stessi (ovvero la loro trasformazione in forma anonima) al termine del trattamento;
- rispettare le procedure di autenticazione informatica e di gestione delle credenziali di autenticazione predisposte da CSBALB;
- rispettare le procedure adottate per garantire l'attività di back up e la custodia di copie di sicurezza, salvando i documenti nelle specifiche cartelle di rete a ciò riservate;
- custodire in modo riservato (e per i dati sensibili o giudiziari in maniera separata e in archivi chiusi a chiave) banche dati e comunque ogni documentazione raccolta nello svolgimento dell'attività lavorativa;
- adottare cautele organizzative per garantire che tutte le persone con cui si collabora siano informate sulle regole di riservatezza adottate per proteggere i dati e seguire le istruzioni fornite per evitare abusi per negligenza, imprudenza o imperizia;
- verificare sempre l'origine dei dati utilizzati;
- segnalare Responsabile della UOSI Sistemi Informativi qualsiasi anomalia riscontrata sui sistemi informatici o nella qualità dei dati presenti nel proprio data base;
- attenersi alle istruzioni che sono state e che verranno impartite (mediante apposite lettere di autorizzazione) per garantire la corretta gestione dei dati stessi.

<u>Gestione delle comunicazioni verbali</u>

Durante l'attività lavorativa è consuetudine scambiare comunicazioni e informazioni in forma verbale, pertanto si rivela necessario tenere in considerazione i seguenti principi:

- nel corso di conversazioni di lavoro occorre tutelare le informazioni coerentemente con il loro livello di classificazione e criticità;
- lo scambio di informazioni concernente l'attività lavorativa deve avvenire all'interno di aree che consentano il mantenimento di adeguati livelli di riservatezza;
- tali aree devono rimanere chiuse durante lo svolgimento di riunioni, conversazioni telefoniche, ecc., rilevanti per l'attività del CSBALB;
- nel corso di conversazioni telefoniche, qualora non risulti strettamente necessario, è preferibile non fare ricorso al sistema viva voce. Nel caso debba essere utilizzato tale sistema, l'interlocutore deve essere avvisato prima della sua attivazione;
- prima di condividere verbalmente dati ed informazioni di lavoro occorre accertarsi che la propria controparte, date le mansioni e le responsabilità assegnate, sia autorizzata a venirne a conoscenza;
- coloro che sono stati provvisti di un telefono cellulare devono cercare di garantire il massimo riserbo sulle proprie comunicazioni; ciò con particolare attenzione al caso in cui vengano ricevute telefonate in aree affollate, in special modo all'esterno della sede del CSBALB.

E. DOCUMENTAZIONE CARTACEA

La documentazione cartacea viene spesso sottovalutata rispetto ai file presenti sul proprio PC. La riduzione del numero di fogli stampati rappresenta un grande obiettivo dal punto di vista della salvaguardia delle risorse naturali, ma anche un ottimo sistema per proteggere l'accidentale diffusione di informazioni.

In tale direzione, il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) prescrive all'art. 40 l'obbligo di creazione e gestione dei documenti originali della Pubblica Amministrazione in modalità informatica.

Si ricordano a titolo esemplificativo alcune misure utili a proteggere la riservatezza e la disponibilità delle informazioni in formato cartaceo:

- fare ricorso alla stampa solo in caso di reale necessità e comunque il meno possibile;
- in caso di stampa ritirare immediatamente i documenti stampati;
- non lasciare mai incustoditi sul proprio tavolo documenti riservati, anche in caso di assenza breve. In generale riporli in contenitori sottochiave o distruggerli in modo sicuro quando non più utili;
- la distruzione dei documenti in modo sicuro avviene con i "raccoglitori di carta" o strappandoli in piccoli pezzi. Evitare in ogni caso di gettare i documenti interi nel cestino dei rifiuti o del riciclo;
- i documenti devono essere controllati e custoditi dagli utilizzatori fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate negli appositi archivi;
- al termine della giornata lavorativa la propria postazione di lavoro deve essere sgombra da tutti i documenti di tipo riservato e da quelli ad uso interno nel caso il posto di lavoro non si trovi in un'area riservata al proprio dipartimento.

F. CONTROLLI INDIRETTI

Controlli

Il CSBALB si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli difensivi e/o indiretti - mirati e non massivi - che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni, mediante l'ausilio di personale tecnico interno o esterno appositamente autorizzato. I controlli possono scaturire anche dall'inefficienza dimostrata dal dipendente nello svolgimento della propria attività lavorativa.

La verifica circa il rispetto del presente Regolamento sarà effettuata anche attraverso gli "strumenti" affidati al personale dipendente per rendere la prestazione lavorativa e per esclusive finalità organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del CSBALB e della riservatezza degli interessati (es. pazienti, dipendenti).

Le informazioni raccolte potranno essere utilizzate per tutte le finalità connesse al rapporto di lavoro e – nel caso di comportamenti contrari a quanto indicato nel presente Regolamento - essere utilizzate anche per l'applicazione di eventuali provvedimenti disciplinari. Per strumento di lavoro si intende – a titolo esemplificativo - l'utilizzo di internet, della mail, del cellulare/tablet istituzionale (per verifica degli accessi internet, della posta elettronica, etc.).

Il Responsabile della UOSI Sistemi Informativi, nel caso sia necessario procedere a un controllo su incarico del titolare e per garantire la piena sicurezza della Rete o per motivi di manutenzione, si riserva di superare ogni accesso e limitazione predisposta (ad esempio password) su computer, account e-mail, dischi di rete, server, etc.

Le verifiche di eventuali situazioni anomale avverranno attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (e-mail, file, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server aziendali attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (reparto, servizio, ecc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;

- in caso di successivo permanere di una situazione non conforme, è possibile procedere con una analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Pertanto, i controlli - proporzionati e non eccedenti anche rispetto allo scopo di verifica dell'adempimento contrattuale - non potranno mai svolgersi direttamente e in modo puntuale, ma saranno preliminarmente compiuti su dati aggregati, riferiti all'intera UO o a suoi Uffici.

A seguito di detto controllo anonimo, potrà essere emesso un avviso generalizzato di rilevazione di eventuali anomalie nell'utilizzo dei presidi tecnologici e con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. Se a detta comunicazione non dovessero seguire ulteriori anomalie, CSBALB non procederà a ulteriori controlli su base individuale e non saranno comunque ammessi controlli prolungati, costanti o indiscriminati.

In caso contrario, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni e a, seconda della gravità della violazione perpetrata, la sanzione prevista potrà prevedere o un semplice richiamo verbale o il divieto temporaneo o permanente dell'utilizzo di strumenti informatici, sino ad arrivare alla risoluzione del rapporto di lavoro, limitatamente alle ipotesi di gravi violazioni e condotte illecite indicate nell'allegato A al presente Regolamento.

Qualora, ad esito di controllo, il Responsabile della UOSI Sistemi Informativi rilevi delle anomalie sull'utilizzo dei sopracitati strumenti informatici che possano essere configurate quali attività non conformi, provvederà ad informare il Direttore Generale e le Direzioni competenti.

Nei casi di accertata violazione dei principi fissati nelle presenti norme generali, è prevista anche l'applicazione dei provvedimenti disciplinari come in seguito specificato, con le modalità ivi previste per il personale dipendente o equiparato e l'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti. Il CSBALB procederà altresì a segnalare l'abuso all'Autorità competente.

<u>Teleassistenza</u>

Relativamente alle attività di manutenzione remota su personal computer connessi alla rete aziendale, il personale tecnico della UOSI Sistemi Informativi potrà utilizzare specifici software.

Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene in accordo con l'utente interessato. La configurazione del software prevede che venga espressamente chiesta l'autorizzazione all'Utente per l'accesso all'attività di manutenzione da parte del servizio tecnico, (un indicatore visivo sul monitor dell'Utente indica quando il tecnico è connesso al personal computer).

Viene fornita, su richiesta, una comunicazione informativa sullo strumento utilizzato nonché le modalità del suo utilizzo per tutti gli utenti aziendali interessati.

G. FORMAZIONE E AWARENESS

La prima misura di sicurezza per la protezione delle informazioni aziendali è indubbiamente la preparazione e consapevolezza del personale dipendente nello svolgere il proprio lavoro in modo sicuro.

Consapevolezza e preparazione sono aspetti che fanno parte del background del personale dipendente, ma che possono essere sviluppati anche attraverso la formazione nelle varie fasi della vita lavorativa (corsi di inserimento e richiami periodici).

Sono state previste sessioni formative e aree dedicate alla formazione. In tali aree si potranno reperire varie risorse per accrescere le proprie competenze e di riflesso migliorare la gestione delle informazioni aziendali.

Periodicamente si procede a interventi formativi specifici per tutti coloro che trattano dati personali e che sono stati istruiti mediante lettera di autorizzazione al trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure organizzative e di sicurezza adeguate adottate dal CSBALB.

La formazione viene programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Referente Privacy Aziendale (DPO Data Protection Officer) ed il Responsabile del Trattamento dei Dati personali sono il punto di contatto per tutto il personale dipendente e gli Utenti (interni ed esterni) per le attività che riguardano e impattano sul trattamento dei dati personali ed a disposizione per qualsiasi dubbio o segnalazione.

Si ricorda che i corsi di formazione previsti non sono facoltativi e che la mancata ed ingiustificata assenza può portare a provvedimenti di tipo tecnico-disciplinare.

H. RESPONSABILITA’

Ogni Utente è responsabile, civilmente e penalmente, del corretto uso delle risorse Informatiche, dell’utilizzo dei servizi e programmi ai quali ha accesso e dei dati personali che tratta.

L’assegnazione di risorse informatiche aziendali non ne comporta il possesso, in quanto trattasi di strumenti di esclusiva proprietà aziendale. Gli Utenti interni utilizzano, nel proprio lavoro, soltanto strumenti informatici assegnati dal CSBALB.

L’uso di computer privati deve essere preventivamente autorizzato dal Responsabile della UOSI che ne verifica la relativa sicurezza.

Per motivi di sicurezza e protezione dei dati, oltre che per ottemperare alle normative vigenti, ogni attività svolta con il Sistema Informatico Aziendale è sottoposta a registrazione in appositi file (log) con riferimento alle credenziali dell’utente e alla stazione di lavoro utilizzata.

Detti file possono essere utilizzati per attività di monitoraggio e controllo del buon funzionamento del Sistema Informatico Aziendale da parte degli Amministratori di Sistema, e possono essere messi a disposizione della Direzione Aziendale e dell’Autorità Giudiziaria nei casi previsti dalla normativa.

La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal Regolamento UE 2016/679 e dal D.Lgs. 196/2003 e s.m.i.

Ciascun Dirigente di U.O. ha la responsabilità di vigilare e verificare il corretto utilizzo degli strumenti informatici assegnati alla propria U.O. e di evitare l’uso improprio o l’accesso da parte di personale non autorizzato, richiedendo all’U.O.C. Informatica gli eventuali interventi necessari.

I. SANZIONI E PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento sono perseguibili con provvedimenti disciplinari individuati nel CCNL vigente, nonché, nei casi più gravi, con azioni civili e penali.

E' comunque immediatamente applicato, a scopo cautelativo, il temporaneo divieto di utilizzo di strumenti informatici.

Prima di assumere qualsiasi decisione disciplinare per un uso non corretto degli strumenti informatici, della mail aziendale o di internet per fini personali, tuttavia, il dipendente sarà invitato a motivare la ragione di tale utilizzo.

La non osservanza del presente Regolamento e disposizioni ivi presenti può comportare, oltre alle sanzioni disciplinari, anche sanzioni civili e penali.

Si precisa inoltre che, ai fini disciplinari, le presenti disposizioni e procedure operative interne, oltre a essere state pubblicate sulla Intranet aziendale – l'Azienda Informa, sono disponibili nel sito web aziendale – sezione privacy e in Amministrazione Trasparente, ai sensi dell'art. 7 della Legge 20 maggio 1970 n. 300.

J. DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

Qualora CSBALB intenda apportare modifiche al presente Regolamento, queste saranno applicate dandone conoscenza immediata al Personale mediante apposita circolare di servizio ed altre modalità.

Qualora si renda necessario per qualsiasi motivo, derogare ad uno o più punti del presente Regolamento, salvo i casi in cui le deroghe siano espressamente previste e disciplinate nello stesso Regolamento, sarà obbligatorio porre per iscritto e veder accettata dal Personale e da CSBALB tale deroga mediante sottoscrizione di entrambe le parti.

Deroghe o modifiche di uno o più punti del presente Regolamento, non rendono invalidi gli altri punti, salvo ipotesi di evidente incompatibilità, per cui prevarrà l'applicazione della clausola temporalmente più recente.

Eventuali comportamenti non in linea con il presente Regolamento, che venissero comunque tollerati da CSBALB non costituiscono una rinuncia della stessa ad esercitare successivamente i suoi diritti per far valere il presente Regolamento.

Il Titolare del Trattamento
Centro Servizi Benedetto Albertini

Il Data Protection Officer
Centro Servizi Benedetto Albertini

ALLEGATO A

ELENCO DELLE CONDOTTE ILLECITE VIETATE E ASSOGGETTABILI A SANZIONE DISCIPLINARE, ANCHE NEGLI ESTREMI DEL LICENZIAMENTO, E LEGALMENTE PERSEGUIBILI:

a) Navigazione intenzionale all'interno di siti web pornografici o pedo-pornografici, detenzione di files di tale natura e/o loro scambio con soggetti terzi (sanzione: Licenziamento);
b) Utilizzo intenzionale della rete aziendale ai fini di:
    i. creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
    ii. creare e conservare su sistemi e supporti informatici aziendali immagini, documenti, dati a carattere privato e non attinenti all'attività lavorativa;
    iii. danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password) e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy (sanzione: Licenziamento);
    iv. effettuare di qualsiasi tipo di attività volta a raggirare o compromettere i meccanismi di protezione dei sistemi informativi (sanzione: Licenziamento);
    v. sfruttare qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi al fine di commettere azioni illecite o non autorizzate (sanzione: Licenziamento);
    vi. falsificare la propria identità (sanzione: Licenziamento);
    vii. svolgere sulla Rete ogni altra attività vietata dalla Legge dello Stato e dalla normativa Internazionale (sanzione: Licenziamento).
c) Download intenzionale da internet di files non correlati all'attività lavorativa e per i quali derivi un danno in capo al CSBALB, di natura civile e/o penale, quale conseguenza della violazione degli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del *software* e/o dalla l. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore (a titolo esemplificativo: file musicali, film o altro materiale coperto da diritti d'autore);
d) Accesso reiterato e per periodi di tempo complessivamente rilevanti a siti internet di contenuto non attinente all'attività lavorativa, anche dopo avere aziendalmente ricevuto specifici richiami in materia;
e) Comunicazione della password aziendale a terzi, senza a ciò essere stati preventivamente autorizzati, nell'ipotesi che da tale comunicazione deriva un danno al CSBALB;
f) Comunicazione/distribuzione/diffusione a terzi documenti classificati come "RISERVATI", ricevuti via mail o con altro mezzo, senza un'autorizzazione scritta del proprietario\creatore del documento\file o del Titolare del trattamento;
g) Copiare qualsiasi dato o file aziendale ovvero comunicare o diffondere all'esterno dati o file aziendali, soprattutto se "Ad uso interno" o "Riservati", in assenza di una preventiva autorizzazione.