Titolo	**Regolamento d'uso della postazione di lavoro e degli strumenti informatici**	
Data emissione	20 maggio 2020	
Data decorrenza	20 maggio 2020	
Da revisionare entro il	30 giugno 2022	
		Firma
Redatto da:	**Organization**	L Garrafa
Verificato da:	**Information & Communication Technology**	G. A. Martinengo
	Human Resources	M. Gastaldi
	Organization	A. Ferrando
	Corporate & Legal Affairs	A. Navarra
Approvato da:	**Human Capital & ICT** **Referente del trattamento dei dati personali per il Gruppo ERG**	G. Coraggioso
Note:	Originale archiviato da Organization	

Versione/Revisione	Data	Principali modifiche
V.1	27/12/2017	
V.2	20/05/2020	• Inserito punto relativo allo Smart Working; • Adeguata indicazione sull'utilizzo del "basket dati" per dispositivi mobili e inserito aspetto relativo al monitoraggio del traffico; • Inserite modifiche relativamente alla "retention" della posta elettronica per personale in uscita con relativi tempi di conservazione, stabiliti in accordo con HR

INDICE

1. Premessa

L'uso improprio della postazione di lavoro (PC, Laptop, Telefono ed ogni altra dotazione informatica) e delle risorse aziendali utilizzate nell'ambito dell'attività lavorativa espone ERG (nel prosieguo, la "**Società**" o "**ERG**") e l'intero Gruppo ERG ai rischi di un coinvolgimento in responsabilità sia di natura patrimoniale che penale, creando potenzialmente problemi di sicurezza ed immagine.

Premesso che l'utilizzo delle risorse aziendali deve sempre ispirarsi al principio della diligenza e correttezza, il Gruppo ERG, a tutela propria e dei propri dipendenti e collaboratori, ha adottato il presente documento (di seguito, il "**Regolamento**") anche per contribuire alla massima diffusione della cultura della sicurezza e per evitare, altresì, che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

2. Scopo

Scopo del presente documento è definire un insieme di norme comportamentali a cui tutti i dipendenti e le terze parti che operano per il Gruppo ERG devono uniformarsi, per garantire le esigenze di protezione delle informazioni, in conformità con i principi generali di ragionevolezza e di collaborazione nella conduzione delle attività aziendali.

Ulteriore scopo del presente documento è assicurare che gli utenti dei sistemi informatici del Gruppo ERG acquisiscano piena consapevolezza e comprensione delle regole in vigore in merito all'accesso ed utilizzo dei sistemi e dei servizi informatici messi a loro disposizione e rispettino le disposizioni di legge vigenti nonché le disposizioni emanate dalle varie Autorità competenti, in relazione all'uso corretto di Internet e della posta elettronica.

3. Ambito

Il presente Regolamento deve essere osservato da chiunque, a qualsiasi titolo, utilizzi dotazioni o servizi informatici forniti da ERG, salvo specifico esonero, in tutto o in alcune parti, da parte di Head of Human Capital & ICT.

4. Riferimenti

- Riferimenti esterni:
  - Codice civile artt. 2086, 2087 e 2104
  - Legge 300/1970 - Statuto dei lavoratori
  - Regolamento generale per la protezione dei dati personali UE 679/2016 (anche denominato "**GDPR**")
  - D. Lgs. 196/2003 – Codice in materia di protezione dei dati personali (Codice Privacy), come successivamente modificato e/o integrato
- Riferimenti interni:
  - Codice etico del Gruppo ERG
  - Modelli di Organizzazione e Gestione ex D. Lgs. 231/2001 eventualmente adottati dalle società del Gruppo ERG
  - Linea Guida "Gestione della Sicurezza delle Informazioni"
  - Linea Guida "Classificazione e protezione delle informazioni"
  - Linea Guida "Procedura di Gestione degli incidenti informatici"

5. Regole di utilizzo della postazione di lavoro e degli strumenti informatici

Gli strumenti informatici sono costituiti dall'insieme delle risorse informatiche aziendali, ovvero dalle risorse infrastrutturali e applicative nonché dal patrimonio informativo digitale.

Le risorse infrastrutturali e applicative sono costituite dalle componenti hardware e software.

Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale comprende tutti i documenti prodotti tramite l'utilizzo delle risorse infrastrutturali e applicative.

Ciascun utente è responsabile, pro quota, dell'utilizzo degli strumenti informatici.

5.1 Informazioni digitali

Si rimanda alla "Linea Guida classificazione e protezione delle informazioni".

5.2 Clean Desk

Si rimanda alla "Linea Guida classificazione e protezione delle informazioni".

Il personale (dipendente e non) deve gestire la documentazione di lavoro minimizzando i rischi inerenti all'accesso non autorizzato, alla diffusione od alla perdita di informazioni riservate. Pertanto, è necessario che vengano rispettate le seguenti direttive:

- sulle scrivanie devono essere posizionati esclusivamente i documenti relativi alle attività in corso: ogni altro materiale deve essere custodito nel rispetto dei criteri di sicurezza e riservatezza;
- nessun documento riservato deve essere lasciato incustodito, nemmeno nel caso di brevi allontanamenti dalla propria postazione di lavoro;
- al termine della giornata lavorativa qualsiasi documento contenente dati personali e/o informazioni confidenziali deve essere riposto in modo da non essere accessibile a personale non autorizzato alla visione;
- in caso di ingresso di estranei nei locali, il dipendente ha l'obbligo di celare ogni informazione personale presente su materiale cartaceo o sullo schermo del proprio computer;
- tutti i documenti devono essere immediatamente recuperati dalle stampanti, dai fax e dalle fotocopiatrici specialmente quelle di rete;
- eventuali documenti non più necessari devono essere eliminati mediante l'uso delle apposite apparecchiature distruggi documenti e, comunque, devono essere resi illeggibili;
- qualora ci si trovi ad operare al di fuori del luogo di lavoro (in smart-working da casa, oppure in mobilità in occasione di trasferte ecc) ed a maggior ragione in luoghi pubblici (sale d'attesa, mezzi di trasporto, ecc.) deve essere prestata massima attenzione affinché nessun estraneo abbia la possibilità di vedere la documentazione gestita, avendo cura di orientare il computer portatile in modo opportuno ed evitando di lasciare in vista eventuale documentazione cartacea.

5.3 Credenziali di accesso

ERG, ove ritenuto opportuno in base alla criticità dei dati e delle informazioni, ha adottato opportuni sistemi che impediscono accessi indebiti da parte di utenti non autorizzati e sistemi di *alert* che segnalano alle UO competenti eventuali comportamenti anomali.

In particolare, al fine di limitare l'accesso alla rete aziendale ed ai sistemi, vengono assegnati all'utente un codice identificativo personale (username o user id) e una parola chiave (password), che costituiscono dati aziendali strettamente riservati. Pertanto:

- l'username di accesso alla rete aziendale è attribuito e gestito da UO ICT che crea una singola utenza digitale per ogni persona. Tale utenza digitale serve per identificare univocamente ogni utente che accede alle risorse ed alle applicazioni informatiche aziendali; successivamente vengono assegnati a tale utenza gli opportuni privilegi di sistema che permettono di accedere alle sole informazioni necessarie per svolgere il proprio ruolo lavorativo;
- l'utilizzo delle credenziali d'accesso personali è responsabilità di ciascun utente;
- non è consentito comunicare le proprie credenziali di accesso a terzi, ivi compresi i propri familiari o persone vicine, seppure in posizione apicale nell'azienda;

- qualora vi sia il sospetto o timore di un utilizzo non autorizzato delle proprie credenziali di accesso, è necessario segnalare immediatamente la sospetta violazione ad ICTsecurity@erg.eu e 3777@erg.eu, nonché provvedere a cambiare la password;
- è necessario che ciascun utente eviti la conservazione di una copia (in chiaro) della propria password su un file o su un supporto cartaceo facilmente accessibile a terzi, nonché il riutilizzo o la copia delle credenziali aziendali per creare altri account personali.

Regole per la generazione ed assegnazione delle credenziali d'accesso:

- il codice identificativo personale (username) deve essere univocamente assegnato ad ogni utente. In particolare, lo username è composto da [iniziale del nome + cognome]. ;
- la prima password deve essere generata in maniera casuale/randomica;
- la password deve essere consegnata all'utente in maniera sicura;
- al primo accesso a seguito di nuova assegnazione, la password iniziale deve essere obbligatoriamente modificata.

Regole per costruire la password:

Nella costruzione della password personale devono essere rispettati, nei limiti dei vincoli tecnici eventualmente esistenti sui diversi sistemi, i seguenti criteri:

- deve essere diversa dallo username o user ID (non deve contenere in tutto o in parte il nome, cognome e lo user dell'utente);
- deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui ciò non sia possibile, ad un numero di caratteri pari al massimo consentito;
- deve essere composta da caratteri maiuscoli e minuscoli, da numeri e da caratteri speciali;
- deve essere diversa dalle ultime 5 versioni precedentemente utilizzate;
- non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
- non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere), tratta da informazioni personali;
- non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti o più di tre caratteri contigui sulla tastiera;
- non deve essere utilizzata per l'acceso alle applicazioni aziendali la stessa password utilizzata per l'accesso a sistemi gestiti da altre organizzazioni

Regole per custodire la password:

La sicurezza della password, oltre che dalla bontà della sintassi di costruzione dipende dall'attenzione con cui viene custodita; pertanto ogni chiave d'accesso:

- deve essere nota esclusivamente all'utilizzatore e non deve essere comunicata ad altri utenti;
- non deve essere scritta su post-it, visibili sulla scrivania o applicati altrove;
- non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione Internet.

Regole per cambiare la password:

Oltra che dalla sintassi e dalle modalità di conservazione, la sicurezza di una password dipende anche dal suo periodo di validità e pertanto la password:

- deve essere obbligatoriamente cambiata in occasione del primo utilizzo e successivamente almeno ogni sei mesi;
- deve essere cambiata immediatamente nei seguenti casi:
  - quando si sospetti che qualcuno ne sia venuto a conoscenza;
  - dopo aver effettuato remotamente l'accesso ai sistemi informativi aziendali attraverso un PC "pubblico" o condiviso (es: Internet Cafè, Wi-Fi pubbliche);
  - a seguito di furto/smarrimento di qualche dotazione aziendale;
- in generale, in qualsiasi occasione in cui si possa ritenere che abbia perso i requisiti di riservatezza.

La password può essere sostituita con una nuova anche prima della scadenza, da parte della UO ICT, per motivate necessità e previa informazione all'utente. In questo caso essa deve essere nuovamente modificata al primo accesso da parte dell'utente.

Per effettuare il reset/sblocco della password deve essere utilizzato lo strumento di self-service aziendale laddove abilitato. In tutti gli altri casi l'utente deve contattare l'Help Desk attraverso i canali predisposti (telefono, e-mail); verificata l'identità del richiedente l'Help Desk provvede a reset/sblocco.

Tutti i possessori di utenza e password sono responsabili di eventuali manomissioni, utilizzi impropri o divulgazioni non autorizzate e sono conseguentemente passibili delle eventuali sanzioni disciplinari/legali del caso.

5.4 Postazioni di lavoro fissa

Per postazione di lavoro fissa si intende il complesso unitario di Personal Computer (di seguito, PC), accessori, periferiche (es. monitor, mouse ecc.) fornito dall'azienda all'utente e tramite il quale viene svolta normalmente l'attività lavorativa.

Ogni PC (accessori e periferiche incluse) sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'azienda ed è fornito all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti all'attività svolta.

Pertanto, devono essere rispettate le seguenti regole:

- è necessario utilizzare responsabilmente e professionalmente le postazioni di lavoro fisse affidate dall'azienda;
- non è consentito effettuare autonomamente cambiamenti o modifiche alla configurazione hardware o software della postazione di lavoro fisse ma le richieste relative a tali modifiche devono essere indirizzate alle strutture aziendali di competenza;
- non è consentito lasciare le postazioni di lavoro fisse incustodite e con le sessioni utenti attive quando ci si allontana dalla propria postazione di lavoro, ma è necessario bloccarle con password o effettuare la disconnessione dalla sessione, anche con l'ausilio di uno screensaver con password;
- non è consentito consumare cibi e bevande in prossimità delle postazioni stesse, per ridurre i rischi di danneggiamento e/o malfunzionamento;
- non è consentito alterare o rimuovere componenti hardware/software.

5.5 Postazioni di lavoro portatili

Le postazioni di lavoro portatili comprendono l'insieme degli strumenti informatici forniti dal Gruppo ERG al fine di svolgere le proprie mansioni lavorative anche al di fuori della sede di lavoro (es. notebook, tablet ecc.).

Gli utenti devono proteggere le postazioni di lavoro portatili fornite dal rischio di furto o di perdita, in seguito ai quali, oltre a cagionarsi un danno all'azienda in relazione al valore del computer stesso, possono concretizzarsi minacce alla disponibilità ed alla riservatezza dei dati, poiché i documenti eventualmente memorizzati (temporaneamente e come eccezione alla regola) sul disco fisso possono entrare nella disponibilità di terzi.

Pertanto, è necessario che vengano adottate le seguenti soluzioni di sicurezza:

- non è consentito lasciare incustodita la postazione di lavoro portatile, né affidarla in custodia a strutture e/o persone non specificamente preposte alla custodia di oggetti di valore (per esempio, non consegnare il dispositivo agli addetti al guardaroba di alberghi, ristoranti, ecc.);
- non è consentito lasciare le postazioni di lavoro portatili con le sessioni utenti attive quando ci si allontana dalla propria postazione di lavoro, ma è necessario bloccarli attraverso l'utilizzo di password o effettuare la disconnessione dalla sessione, anche con l'ausilio di uno screensaver con password.

L'utente è responsabile del dispositivo assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro o remotamente. Pertanto, è necessario seguire le seguenti regole:

- le postazioni di lavoro portatili utilizzate all'esterno (attività di lavoro fuori sede in occasione di convegni, corsi esterni, ecc), in caso di allontanamento, devono essere custodite in un luogo protetto (ed esempio, non è consentito lasciare la postazione di lavoro portatile in automobile durante le soste, neppure nel bagagliaio e in caso di viaggi aerei è necessario trasportare la postazione di lavoro portatile come bagaglio a mano e sistemarlo in una custodia adeguata). Al di fuori degli uffici aziendali, laddove realmente opportuno, è necessario utilizzare il cavo di sicurezza per bloccare fisicamente la postazione di lavoro portatile a un supporto fisso (ad esempio alle scrivanie);
- i dati eventualmente archiviati in locale sulle postazioni di lavoro portatili (temporaneamente e come eccezione alla regola) devono essere protetti in base a quanto previsto dalla *LG Classificazione e protezione dei dati.*
- alle postazioni di lavoro portatili si applicano le regole di utilizzo previste per le postazioni di lavoro fisse connesse in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. Parimenti i dati contenuti nei dispositivi rimovibili devono essere cancellati prima della riconsegna degli apparati;
- in caso di smarrimento o furto di un dispositivo, l'assegnatario deve segnalare immediatamente l'accaduto a UO ICT, per le opportune pratiche assicurative e deve presentare quanto prima copia della denuncia sporta presso le autorità competenti.

5.6 Software

I Software rappresentano tutti i programmi installati sui dispositivi fisici delle postazioni di lavoro o di altri strumenti hardware. Rappresentano gli strumenti con cui vengono generati/manipolati i dati e le informazioni aziendali.
Pertanto, è necessario che vengano rispettate le seguenti regole di sicurezza:

- non è consentito tentare o effettuare autonomamente aggiunte o modifiche alla configurazione software standard fornita dall'azienda, ma le richieste relative a tali modifiche devono essere indirizzate alle strutture aziendali di competenza;
- non è consentito installare software per uso personale sulle postazioni di lavoro aziendali (fisse/portatili): tale azione può comportare l'introduzione e la propagazione di virus all'interno dei sistemi aziendali o l'utilizzo di software non conformemente alle regole di licenza sotto cui è stato rilasciato;
- non è consentito prelevare software da Internet o copiati da dispositivi esterni;
- non è consentito installare ovvero eseguire sulle postazioni di lavoro aziendali (fisse/portatili) software senza licenza (es. software copiati illegalmente), nonché modificare programmi esistenti su dispositivi elettronici aziendali, riprodurre o duplicare i programmi informatici;
- è necessario utilizzare il software entro i limiti specificati nei contratti di licenza;
- è vietato copiare i software resi disponibili dall'azienda (sia sviluppati internamente sia con licenza, salvo i casi espressamente autorizzati in virtù di specifici accordi con i vendor) su memorie esterne usb o su altri supporti di memorizzazione;
- è vietato installare software in violazione delle regole di copyright o di altri diritti di proprietà intellettuale (es. musica, file, foto, video ecc.).

5.6.1 Antivirus

La possibilità che si riescano a prevenire infezioni da virus informatico non dipende solo dalla presenza di adeguati strumenti a ciò dedicati e dalla loro corretta configurazione, ma anche e soprattutto dalle modalità di utilizzo degli stessi.
Pertanto, è necessario seguire le seguenti direttive:

- non è consentito modificare la configurazione né disabilitare, per qualsiasi motivo, il sistema antivirus;
- non è consentito utilizzare prodotti antivirus diversi da quelli forniti dall'azienda;

- è necessario segnalare tempestivamente all'UO ICT eventuali malfunzionamenti del sistema antivirus;
- è necessario segnalare tempestivamente all'UO ICT la presenza di virus riconosciuti dal sistema antivirus e non autonomamente rimossi dal sistema stesso.

5.7 Dispositivi di memorizzazione portatili

Per dispositivi di memorizzazione portatili si intendono tutti quei dispositivi (es.CD-ROM, DVD, dispositivi di memorizzazione USB, riproduttori musicali MP3, fotocamere, ecc.) che consentono di copiare o archiviare dati, file o documenti all'esterno delle postazioni di lavoro aziendali.
Pertanto, è necessario seguire le seguenti regole:

- non è consentito utilizzare dispositivi di memorizzazione portatili personali, se non preventivamente autorizzati dall'azienda;
- ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'azienda, i dispositivi devono essere gestiti secondo quanto previsto dal presente documento;
- i supporti di memorizzazione, quando mantenuti all'interno di una delle sedi aziendali, devono essere custoditi in archivi ad accesso limitato al solo personale autorizzato;
- non è consentito portare all'esterno dell'azienda i dispositivi di memorizzazione portatili senza aver applicato le misure di sicurezza necessarie previste dalla *LG Classificazione e protezione dei dati*.

5.8 Stampanti, fotocopiatrici e fax

Le stampanti, le fotocopiatrici e i fax sono strumenti informatici aziendali e devono essere utilizzati dal personale esclusivamente per attività di carattere lavorativo, non per scopi di natura personale e ponendo particolare attenzione alla minimizzazione del numero di stampe prodotte.
Pertanto, è necessario durante l'utilizzo delle stesse, rispettare le seguenti regole:

- è necessario ritirare immediatamente i documenti stampati che non devono essere lasciati incustoditi sulla stampante;
- è necessario stampare tutte le informazioni di natura particolarmente riservata esclusivamente su stampanti presenti all'interno delle sedi aziendali o in uffici in cui l'utente sia autorizzato al trattamento dei medesimi dati;
- qualora ci si accorga di aver commesso un errore nella stampa, è necessario procedere all'annullamento della stampa;
- qualora non si riesca ad annullare la stampa e ci si accorga, al momento del ritiro della stampa, di errori che rendono inutilizzabili i documenti, è necessario provvedere alla distruzione dei medesimi nei propri uffici;
- le copie possono essere consegnate solo ad utenti autorizzati a trattare la determinata tipologia di dati contenuta nei documenti;
- qualora vengano effettuate copie di documenti contenenti dati sensibili, non ci si deve allontanare dalla stampante durante la copiatura, per evitare che altri utenti non autorizzati entrino in contatto con i documenti.

L'invio e la ricezione di fax devono seguire le seguenti prescrizioni:

- è necessario garantire la massima riservatezza delle informazioni proteggendo, per quanto possibile, il documento da sguardi indiscreti;
- è necessario che gli utenti riportino in ufficio sia il documento inviato sia il "rapporto di trasmissione" e si assicurino, qualora il dispositivo del fax non sia nel proprio ufficio, di non lasciare nulla presso l'ufficio ove è stato inviato il fax;
- nel caso della ricezione di fax erroneamente indirizzati, è necessario che gli utenti dell'unità organizzativa destinataria trattino tali documenti con la massima riservatezza in quanto potrebbero contenere dati personali o informazioni riservate appartenenti a terzi soggetti;

- nel caso della ricezione di fax erroneamente indirizzati è necessario che gli utenti non rispondano via fax al numero mittente, bensì verifichino la presenza sul documento ricevuto di un numero telefonico da contattare per avvisare dell'erroneo invio: soltanto dopo aver contattato il mittente o il destinatario del fax è possibile eliminare definitivamente il documento ricevuto, utilizzando un dispositivo trita-documenti.

5.9 Smartphone aziendali

In funzione di specifiche attività lavorative, il Gruppo ERG fornisce ai propri dipendenti un telefono cellulare o smartphone aziendale. I dipendenti possono utilizzare lo smartphone in dotazione anche a titolo personale (assegnazione in uso promiscuo) ponendo in generale una ragionevole attenzione al contenimento della spesa soprattutto nell'uso all'estero e della modalità "hot-spot" a servizio del portatile eventualmente in uso, se abilitati, ed evitando qualsiasi abuso.
Il dispositivo assegnato è di proprietà dell'azienda ed è dato in dotazione prioritariamente per finalità di supporto all'attività lavorativa (fatto salvo l'uso promiscuo); pertanto devono essere rispettate le seguenti regole:

- l'utilizzo appropriato del cellulare è di responsabilità dell'assegnatario dell'apparecchio;
- non è concesso agli assegnatari dei telefoni cellulari aziendali prestarli, noleggiarli o comunque darli in utilizzo a terzi, interni o esterni, non assegnatari;
- la responsabilità rispetto alla cura e all'utilizzo dell'apparecchio è affidata all'assegnatario dello stesso;
- la configurazione con cui il dispositivo è consegnato non deve essere modificata;
- in caso di malfunzionamento o di guasto dell'apparecchio o della Sim il dipendente deve rivolgersi a UO ICT;
- in caso di furto o smarrimento dell'apparecchio il dipendente deve darne immediata comunicazione a UO ICT, ai fini dell'immediato blocco dell'utenza e cancellazione remota del dispositivo. Il dipendente deve quindi presentare la formale denuncia di furto o smarrimento e farne pervenire copia a UO ICT per gli adempimenti successivi. Se il furto o lo smarrimento avvengono in circostanze o in tempi in cui non è possibile comunicare con UO ICT, il dipendente deve seguire la seguente procedura:
  - Verifica tramite Geolocalizzazione della posizione del telefono (attraverso www.icloud.com)
  - Blocco da remoto del telefono (attraverso www.icloud.com):
    "Please return to ERG SpA +3901024011"
  - Formattazione remota (attraverso www.icloud.com)
  - Blocco della Sim contattando il gestore di telefonia mobile
  - Cambio della password di rete (ERG) e di eventuali altre password rilevanti;
- è vietato acquisire i privilegi amministrativi (ad esempio, di root), effettuare il jailbreak o la manomissione dei sistemi operativi dei cellulari aziendali;
- è obbligatorio l'uso del PIN di sicurezza della SIM ed il codice di sblocco del dispositivo secondo quanto impostato centralmente attraverso la piattaforma di "Mobile Device Management" adottata dal Gruppo; in ambedue i casi è vietata la disabilitazione. In particolare, il codice di sblocco deve:
  1. essere di almeno 6 caratteri
  2. non essere in sequenza ascendente o discendente (es. 123456)
  3. non contenere più di 3 volte consecutive lo stesso carattere
  4. essere diverse dal proprio PIN personale
  5. richiedere la ri-autenticazione dopo 1 minuti di inattività;
- la SIM viene consegnata con un profilo telefonico che attinge ad un basket dati condiviso aziendale (per mail, app e internet). Ai fini del rispetto dei budget dei costi nonché per garantire a tutta l'utenza un adeguato livello di servizio, il Gruppo si riserva di:
  - monitorare periodicamente i volumi di traffico generato, segnalando agli utenti le eventuali anomalie rispetto ad un utilizzo normale e congruo considerando le finalità con cui le dotazioni sono assegnate;
  - assegnare a ciascuna utenza, tramite opportune configurazioni tecniche, una quota predefinita di traffico congrua con un normale utilizzo, ed attivare opportuni meccanismi di alert all'utenza in

funzione del livello di traffico raggiunto, bloccando eventualmente e temporaneamente l'utilizzo qualora venga superata in maniera rilevante la soglia di traffico considerata ragionevole;

- la navigazione Internet tramite telefono cellulare / smartphone è soggetta alle regole previste e definite nel relativo paragrafo del presente Regolamento;
- il Gruppo si riserva la possibilità di limitare o inibire, tramite opportuni blocchi o segnalazioni sull'apparecchio, l'installazione di app che non siano coerenti con i principi etici adottati dal Gruppo, che non rispettino normative vigenti o che possano costituire rischi per le funzionalità dell'apparato;
- l'uso di reti wi-fi libere e disponibili è ammesso se ritenute affidabili e sicure, ed è consigliato in caso di scarico di grandi quantità di dati per limitare il consumo del basket dati;
- deve essere posta particolare attenzione alla gestione delle comunicazioni telefoniche in ambienti pubblici (es. locali, stazioni e mezzi di trasporto ecc.), al fine di prevenire la diffusione di informazioni aziendali da parte di terzi non autorizzati.

5.10 Navigazione Internet

L'utilizzo di Internet e la navigazione in rete sono consentite, ai fini dell'attività lavorativa e coerentemente con le mansioni assegnate, salvo diversa indicazione.
L'accesso ad Internet è fornito allo scopo di consentire il reperimento di eventuali informazioni necessarie allo svolgimento dell'attività lavorativa o per accedere ad applicazioni / sistemi web-based. Essendo uno strumento di lavoro, i soggetti cui la Società attribuisce l'accesso sono responsabili del suo corretto utilizzo nel pieno rispetto della normativa di riferimento vigente, nonché secondo normali standard di correttezza, buona fede e diligenza professionale.
L'azienda, con il presente Regolamento, ha inteso definire per gli utenti uno specifico codice di condotta in modo da evitare comportamenti che inconsapevolmente potrebbero, attraverso l'uso improprio, danneggiarla.
In particolare, si devono osservare le seguenti regole:

- è vietata la navigazione su siti contrari all'etica, al buon costume o aventi contenuti illegali;
- è vietato scaricare programmi, anche se privi di licenza o in prova (freeware e shareware), se non in caso di espressa autorizzazione da parte della UO ICT; eseguire il download di file da Internet è, infatti, un'operazione intrinsecamente pericolosa in quanto può essere il veicolo per l'introduzione di virus nella rete aziendale;
- è vietato trasmettere o scaricare e installare materiale in violazione di quanto previsto dal copyright;
- è proibito creare, trasmettere, pubblicare e/o archiviare sotto qualunque forma (immagini, testi, filmati, registrazioni vocali ecc.) qualsiasi tipo di materiale:
  - che infranga le leggi sul diritto d'autore e la proprietà intellettuale;
  - che includa contenuti che siano dannosi, minatori, molesti, offensivi, calunniosi o volgari;
  - che violi le leggi sulla Privacy;
  - che incoraggi il compiersi di azioni criminali e che, in generale, possa arrecare danno all'azienda;
- non è consentita ogni forma di registrazione con le credenziali aziendali a siti i cui contenuti non siano legati all'attività lavorativa;
- è vietata la condivisione di file in modalità cd. peer-to-peer;
- è vietato immettere sulla rete o sui server software dannoso per i sistemi o comunque non autorizzato;
- è vietato utilizzare l'infrastruttura tecnologica dell'azienda per procurarsi e diffondere materiale in violazione con le normative vigenti;
- l'utilizzo deve essere conforme ai principi del codice etico di Gruppo e ai principi di correttezza;
- qualsiasi utilizzo per finalità personali (es. partecipazione a social networks, effettuazione di transazioni finanziarie od altre tipologie di acquisto, ecc) deve avvenire nel rispetto di normali criteri di ragionevolezza in termini di tempo e continuità e, comunque, tramite credenziali private.

Il Gruppo, per ridurre il rischio di usi impropri della "navigazione" in Internet ha adottato, dove applicabili, opportune misure che garantiscono il corretto utilizzo dei dispositivi e sistemi aziendali in conformità a quanto previsto nel presente Regolamento; ha provveduto pertanto a configurare i sistemi e ad utilizzare

filtri in modo da prevenire le operazioni reputate non coerenti con l'attività lavorativa come l'accesso a determinate pagine web od a specifiche categorie di siti. Per le medesime ragioni sono impediti l'upload o il download di file aventi particolari caratteristiche di tipologia di dato.

5.11 Strumenti di messaggistica istantanea/Collaboration

Gli strumenti di messaggistica istantanea/collaboration (es. Skype, WhatsApp, ecc.) sono dei sistemi di comunicazione in tempo reale attraverso la rete, tipicamente Internet o una rete locale, che permettono ai suoi utilizzatori lo scambio di brevi messaggi.

L'utilizzo di tali strumenti è consentito a tutti gli utenti al fine di agevolare le comunicazioni tra loro. Pertanto, l'utilizzo di tali strumenti deve avvenire nel rispetto delle seguenti direttive:

- non possono essere scambiate informazioni classificate come CONFIDENZIALI o AD USO INTERNO;
- non devono contenere messaggi di natura sessuale, discriminatoria e diffamatoria e comunque in violazione con le normative vigenti;
- possono essere utilizzate per comunicazioni private con utenti esterni all'ambito aziendale ma unicamente nel rispetto dei limiti di correttezza e misura, ossia non deve essere eccessivo, ossia non deve essere tale da incidere sulle performance lavorative.

5.12 Social network

Rientrano in questo ambito sia l'utilizzo privato di Social Network (es. Facebook, Twitter, Linkedin ecc.) da parte di dipendenti o collaboratori sia l'utilizzo da parte dell'azienda stessa per finalità di natura interna (ad es. comunicazione con i dipendenti, condivisione di informazione all'interno di gruppi di lavoro, etc.) o di business.

Pertanto, l'utilizzo dei Social Network deve avvenire nel rispetto delle indicazioni contenute nella Procedura "Gestione Social Media" ed ai sensi del presente Regolamento.

L'utilizzo deve essere effettuato nel rispetto del disciplinare in materia di posta elettronica ed Internet (Provvedimento Garante Privacy del 1/3/2007).

Il profilo degli utenti, qualora consenta di correlarli all'azienda, deve essere adeguatamente protetto da password e devono essere adottate stringenti impostazioni sulla privacy.

In particolare, gli utenti non devono:

- tentare di accedere a siti o contenuti in cui è presente materiale inappropriato o, comunque, contrario all'etica, al buon costume o avente contenuti illegali;
- rilasciare dichiarazioni denigratorie, pubblicare informazioni o partecipare ad attività che potrebbero diffamare, calunniare o danneggiare la reputazione dell'organizzazione, delle persone e/o delle terze parti che collaborano con l'azienda. Ciò include l'utilizzo, la condotta o il comportamento online e/o sui social media, anche al di fuori dall'ambiente di lavoro;
- usare i social network ed i forum in modo irresponsabile e non in conformità con i principi dell'azienda e le leggi italiane;
- diffondere le informazioni, i documenti e ogni dato personale relativo a clienti, dipendenti o fornitori dell'azienda, ivi comprese informazioni riservate dell'azienda, online, sui social network o forum;
- utilizzare il proprio indirizzo e-mail aziendale per registrarsi a social network e/o forum esterni non attinenti alla attività lavorativa;
- pubblicare, inviare o ricevere volontariamente, caricare/scaricare, ottenere, salvare o condividere qualsiasi contenuto o materiale che infranga, utilizzi in maniera inappropriata, o violi in altro modo i diritti di proprietà intellettuale, privacy o pubblicità di qualsiasi individuo, gruppo o ente.

5.13 Strumenti di conferenza e videoconferenza

Gli strumenti di conferenza o videoconferenza sono ampiamente utilizzati al fine di ridurre i costi di spostamento e velocizzare i processi di business, ma non sono esenti da rischi.

Pertanto, è necessario rispettare le seguenti direttive in materia di sicurezza:

- è opportuno porre attenzione nella trasmissione di informazioni classificate come CONFIDENZIALE;

- i partecipanti alla conferenza/videoconferenza devono essere posizionati in maniera tale da rendere impossibile l'ascolto o la visione della conferenza da parte di terzi non autorizzati (preferibile utilizzare una sala specifica e dedicata alle conferenze);
- nel caso di videoconferenze assicurarsi che la videocamera inquadri solo l'individuo e che il volume del microfono sia al minimo indispensabile per permettere la comunicazione;
- è necessario effettuare un log-on tramite password e un log-off per ogni sessione di conferenza/videoconferenza;
- è necessario verificare che partecipino alla conferenza/videoconferenza solo le persone effettivamente invitate e autorizzate, verificandone l'identità.

5.14 Posta elettronica

Il Gruppo rende disponibili due tipologie di indirizzi di posta elettronica: indirizzi personali (costruiti come <iniziali-del-nome><cognome>@erg.eu) e indirizzi condivisi tra più utenti (ad esempio, <funzioneXYZ>@erg.eu).
La casella di Posta Elettronica assegnata dal Gruppo ERG all'utente ed il relativo indirizzo, nonché i messaggi in entrata ed in uscita dalla stessa, sono di proprietà aziendale. Essi rappresentano uno strumento di lavoro affidato all'utente al solo fine di consentirgli di svolgere l'incarico affidato. Le persone assegnatarie delle caselle di posta elettronica sono pertanto responsabili del corretto utilizzo delle stesse.
L'assegnazione della casella di posta elettronica personale avviene in concomitanza con la creazione dell'utenza al momento dell'assunzione; al momento della cessazione del rapporto di lavoro, l'utenza personale viene automaticamente bloccata e la relativa casella di posta elettronica viene automaticamente cancellata dopo 30 giorni, fatto salvo quanto diversamente previsto nel presente documento.
Relativamente alla posta elettronica dei "Manager & above" o di soggetti il cui ruolo è ritenuto importante per le attività svolte, per cui il mantenimento della posta aziendale è necessario ad assicurare la continuità aziendale, HR deve valutare caso per caso se debba essere mantenuta una copia di back-up dopo l'uscita del Dipendente e comunicarlo esplicitamente ad ICT entro la data di uscita, oltre che al Dipendente in uscita. Il back-up eventualmente archiviato secondo le indicazioni di HR non deve essere reso disponibile a nessuno ad esclusione dell'Head of Human Capital & ICT e/o suoi delegati per le finalità di cui al presente documento. Tale back up può essere fornito al Dipendente prima della sua uscita dietro esplicita autorizzazione di HR. Lo stesso viene conservato per il tempo strettamente necessario a garantire la predetta continuità aziendale.

Regole d'uso della posta elettronica

Devono essere mantenuti comportamenti corretti nell'ambito dell'utilizzo dello strumento di posta elettronica. In particolare, valgono le seguenti regole:

- i messaggi di posta elettronica contenuti nella casella di posta di un utente sono considerati come attinenti allo svolgimento dell'attività lavorativa dallo stesso svolta a favore del Gruppo: a seguito di eventuali eccezionali utilizzi della posta elettronica aziendale per finalità personali gli utenti devono cancellare i messaggi di natura personale dal sistema non appena trasmessi e/o letti;
- non divulgare informazioni riservate a terzi, confidenziali o comunque di proprietà del Gruppo ERG, senza espressa autorizzazione della Società stessa;
- non inviare né conservare messaggi di posta elettronica o più in generale dati, programmi o altro materiale di natura informatica dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;
- tutta la posta entrante è controllata da software antivirus/antimaleware/antispam e una eventuale e-mail infetta viene messa in quarantena e segnalata al destinatario o posta in apposita cartella di sistema dell'utente. È comunque necessario prestare la massima attenzione nell'apertura degli allegati alle mail ricevute, indipendentemente dal fatto che si conosca o meno il mittente in quanto è comunque possibile che alcune mail superino i filtri impostati sul sistema centrale. In particolare, non devono

essere aperti documenti con nomi "anomali", né devono essere aperti file o macro ricevuti in allegato a e-mail provenienti da un mittente sconosciuto o sospetto (in questo caso segnalare immediatamente l'accaduto a UO ICT scrivendo a 3777@erg.eu ed a ICTsecurity@erg.eu);

- non ci si deve connettere a siti web utilizzando link contenuti in e-mail provenienti da un mittente sconosciuto o sospetto, ma bisogna segnalare immediatamente l'accaduto a UO ICT ERG SpA scrivendo a 3777@erg.eu ed a ICTsecurity@erg.eu;
- gli allegati alle e-mail inviate devono avere una dimensione contenuta in modo da non rendere difficoltosa l'attività del mail server aziendale;
- si deve disattivare l'esecuzione automatica di programmi (es. activeX) allegati ai messaggi di posta elettronica;
- inviare messaggi di posta elettronica non desiderati o richiesti, inclusa la spedizione di qualunque informazione pubblicitaria a soggetti che non abbiano specificatamente richiesto tali informazioni (spam), rappresenta una palese violazione alle norme dettate dalla legge sulla privacy. Nel rispetto della predetta norma e di quanto ad essa riconducibile è espressamente proibito agli utenti di utilizzare i mezzi aziendali per:
  - qualunque forma di molestia via e-mail, sia attraverso il contenuto che la frequenza di invio o le dimensioni del messaggio;
  - l'utilizzo non autorizzato dell'intestazione delle e-mail o la creazione di intestazioni false;
  - la creazione o l'inoltro di e-mail appartenenti a catene o similari.
- non vanno utilizzati impropriamente gli elenchi di distribuzione, il cui uso è riservato alle funzioni aziendali preposte;
- occorre limitare il numero di copie distribuite della stessa e-mail. Una comunicazione va naturalmente spedita a tutti gli interessati, mentre in copia va spedita alle altre persone citate nella comunicazione;
- avvalendosi delle funzionalità messe a disposizione dal sistema di posta elettronica, deve essere inserita in calce alla mail la propria firma predefinita secondo lo standard predisposto dall'U.O. Communication e consultabile sulla Intranet. La firma va inserita anche nelle mailbox delle caselle di funzione;
- le strutture aziendali che inviano e/o ricevono comunicazioni di lavoro che possono necessitare di una consultazione da parte di più utenti appartenenti alla struttura stessa, devono fare richiesta per tramite del proprio responsabile di una casella di posta di funzione opportunamente condivisa e protetta (es. <FunzioneXYZ>@erg.eu). Tali caselle garantiscono la continuità operativa in caso di assenza prolungata (es. ferie, maternità, malattia o attività di lavoro fuori sede) o di cessazione del rapporto di lavoro di uno degli appartenenti alla struttura stessa;
- in caso di assenza prolungata e non programmata, l'utente deve altresì avvalersi delle funzionalità messe a disposizione dal sistema di posta elettronica che garantisce ad ogni utente, titolare di una mailbox, la possibilità di:
  - inviare automaticamente, in caso di assenze, messaggi di risposta contenenti esclusivamente il periodo di assenza e le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura di appartenenza;
  - autorizzare la visione del contenuto ad un fiduciario a condizione necessaria che sia provvisto di un account valido sullo stesso dominio. Tale delega può essere impostata utilizzando la funzionalità denominata "delega posta" direttamente dall'utente titolare della casella o per tramite dell'Help Desk.
- non possono essere mantenute attive caselle di posta di un utente in seguito alla sua uscita dal Gruppo ERG per qualsiasi motivo ciò avvenga; per garantire la continuità operativa, i Responsabili di Unità Organizzativa devono organizzarsi con le caselle di funzione condivise. Eccezionalmente, previa valutazione da parte delle U.O. competenti, può essere attivato sul contatto mailbox del collaboratore uscente, per un periodo di 30 giorni massimo, un messaggio di replica automatica contenente le coordinate di un altro soggetto o altre utili modalità di contatto della struttura interessata;

- non è consentito configurare l'accesso alla casella di posta elettronica aziendale sui dispositivi privati fissi e mobili tra cui cellulari, smartphone e tablet. La configurazione dell'accesso determinerebbe, infatti, il download sul dispositivo privato di dati aziendali senza la possibilità per l'azienda di garantirne un adeguato livello di protezione attraverso l'adozione di idonee misure di sicurezza. L'unica modalità di consultazione della posta consentita con tali dispositivi è via browser.

5.15 Richiesta e Consegna degli strumenti informatici aziendali

La richiesta di uno o più strumenti aziendali va fatta secondo quanto indicato dalla Procedura "Assegnazione dotazioni informatiche" ed attraverso il sistema di Gestione delle richieste (SMART).
Successivamente al ricevimento della dotazione l'utente, per i casi in cui si applica, deve chiudere lo SMART relativo, confermando la ricezione del bene ed accettando l'utilizzo secondo il presente Regolamento.

5.16 Restituzione degli strumenti informatici aziendali

Al termine dell'impiego o del contratto lavorativo, deve essere restituito all'azienda ogni strumento fornito o prodotto durante il periodo lavorativo (fatte salve eventuali eccezioni esplicitamente autorizzate da HR e comunicate ad ICT entro la data di cessazione del rapporto di lavoro, anche con riferimento al back-up della casella di posta elettronica), per esempio:

- ogni dispositivo o strumento assegnato per garantire l'accesso fisico (es. Badge, chiavi) o logico (es. token) ai servizi aziendali;
- ogni documento, file, dati, progetti, software (inclusi i codici sorgente), libri o manuali elaborati o redatti dall'utente ai fini della propria attività lavorativa;
- ogni strumento informatico (laptop, telefono cellulare, tablet, usb, hard drive portatili, CD/DVD, ecc.) e/o bene (es. auto) aziendale assegnato.

5.17 Verifiche sull'utilizzo del collegamento ad Internet e della casella di posta elettronica aziendale

L'azienda si riserva la facoltà di effettuare, nel rispetto dei principi di pertinenza e non eccedenza e tramite strumenti che minimizzino il trattamento dei dati personali, le verifiche che ritenga opportune e necessarie per le seguenti legittime finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici;
- assicurare la conformità dell'utilizzo alle leggi e ai regolamenti, nonché evitare la commissione di illeciti;
- vigilare sul corretto utilizzo degli strumenti informatici (inclusa la navigazione Internet e l'uso della posta elettronica, come disciplinati nel presente Regolamento) da parte degli utenti;
- verificare la funzionalità del sistema e degli strumenti informatici, assicurando la continuità del business;
- ove vi sia un sospetto, investigare o identificare usi inappropriati, nonché violazioni del presente Regolamento o di altre policy specifiche dell'azienda o fare valere o difendere i diritti del Gruppo ERG;
- rispondere alle richieste delle autorità competenti.

Nell'effettuare le verifiche per le finalità sopra specificate, l'azienda garantisce l'assenza di interferenze o violazioni ingiustificate dei diritti e delle libertà fondamentali dei soggetti che ricevono o inviano comunicazioni elettroniche di natura personale o privata. L'azienda garantisce altresì che attraverso le seguenti verifiche non sia effettuato alcun controllo a distanza della prestazione lavorativa.
La Società adotta adeguati accorgimenti tecnici (es. filtri, configurazioni di sistemi etc.) per prevenire eventi dannosi o situazioni di pericolo informatico; a fronte di eventuali problemi, la Società si riserva peraltro la facoltà di effettuare le opportune verifiche tecniche sulle anomalie riscontrate, operando analisi su dati aggregati e riferiti all'intera struttura lavorativa o a sue sotto-aree.
Le verifiche aggregate avvengono o periodicamente o per ragioni di evidenza di una anomalia, sono di natura statistica e non sono ricollegabili a comportamenti leciti o illeciti del singolo utente

La verifica aggregata, di sua natura anonima, può concludersi con un avviso generalizzato relativo ad un utilizzo rilevato come "anomalo" degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
Qualora a seguito delle verifiche collettive, dei relativi avvisi o della presenza di altre situazioni di anomalia, possono essere effettuate verifiche su base individuale, nominativi, sui singoli dispositivi e postazioni. In tal caso viene inoltrato, con la dovuta riservatezza, un preventivo avviso individuale alla persona oggetto del controllo con espresse le ragioni legittime della verifica e le modalità tecniche con cui viene effettuata.
Gli unici soggetti autorizzati a svolgere le verifiche sopra indicate sono i seguenti soggetti e/o gli Amministratori di Sistema da loro incaricati:

- Head of Human Capital & ICT anche in qualità di Referente del Trattamento dei Dati Personali;
- Head of Human Resources;
- Head of Information & Communication Technology;
- ICT Governance, Integration & Security;
- ICT Infrastructures & Services;

Ai soggetti preposti corre l'obbligo di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità riconducibili alla ricerca e all'esame di situazioni anomale e alle attività di manutenzione dei Sistemi.
È proibito a soggetti privi dello specifico incarico da parte dell'azienda di effettuare qualunque genere di attività finalizzata al controllo sulla posta elettronica e sull'accesso a Internet, anche per perseguire finalità lecite.
L'elenco degli Amministratori di Sistema è disponibile presso la U.O. Organization.

5.17.1 Verifiche sul rispetto delle modalità di utilizzo di Internet

Per motivi di sicurezza e di gestione tecnica, tutte le connessioni ad Internet richiedono, da parte degli utenti abilitati, l'autenticazione ad un proxy server che registra, in appositi file di log le seguenti informazioni:

- IP e/o nome del PC e/o nome utente che effettua la richiesta;
- Data e ora della richiesta;
- Nome dispositivo, IP e/o indirizzo, porta di destinazione della richiesta;
- Tempo di elaborazione, byte ricevuti, byte inviati,
- Protocollo, metodo HTTP, URL;
- Rete di origine;
- Rete di destinazione

Tali file di log possono essere consultati da soggetti incaricati esclusivamente per motivi di sicurezza interna o su richiesta dell'autorità giudiziaria. In nessun modo possono essere utilizzati per effettuare una profilazione delle abitudini di traffico degli utenti, ivi compresi i siti web visitati, o per un controllo a distanza degli stessi salvo che in dati aggregati ed anonimi.
I report costruiti per effettuare i controlli aggregati sopra descritti sono anonimizzati attraverso l'eliminazione di qualsiasi informazione che permetta l'identificazione immediata dell'utente (nome utente ed IP della postazione che ha originato la richiesta).
I file di log sono conservati per un periodo massimo di 30 giorni decorsi i quali sono cancellati automaticamente (attraverso procedure di sovra-registrazione come, ad esempio, la cd. rotazione dei log file).

5.17.2 Verifiche sul rispetto delle modalità di utilizzo della posta elettronica

Nessuna verifica viene compiuta in maniera regolare sulla Posta Elettronica, né tantomeno alcun controllo viene compiuto sul contenuto delle mail sia in ingresso sia in uscita.

Il Gruppo ERG accede alle caselle di posta elettronica affidate agli utilizzatori nel rispetto dei limiti stabiliti nel presente documento. La Società applica le seguenti modalità di gestione e controllo delle caselle di posta elettronica aziendali:

- le caselle di posta sono soggette ad attività di salvataggio (backup) automatico, che permette di non perdere le informazioni memorizzate anche in caso di incidenti;
- le informazioni relative ai messaggi in entrata ed in uscita dagli indirizzi di posta elettronica aziendale ed i relativi dettagli tecnicamente necessari per svolgere il servizio e-mail vengono registrate e memorizzate all'interno di file di log;
- i log sono conservati per un periodo massimo di 30 giorni e sono cancellati periodicamente ed automaticamente (attraverso procedure di sovra-registrazione come, ad esempio, la cd. rotazione dei log file).

6. Segnalazione incidenti di sicurezza informatica

Gli incidenti di sicurezza informatica sono normati dalla Procedura di Gestione degli incidenti informatici a cui si rimanda.
Ogni utente è tenuto a segnalare tempestivamente al 3777@erg.eu e ad ICTsecurity@erg.eu qualsiasi incidente o anomalia dovesse riscontrare nell'uso degli strumenti informatici in dotazione, nella gestione delle credenziali di accesso o nella navigazione internet e nell'uso della posta elettronica.
La segnalazione tempestiva è prerequisito necessario per garantire rapidità ed efficacia nella individuazione e risoluzione di eventuali compromissioni o violazioni di informazioni riservate, nonché per contrastare possibili attacchi e mitigarne eventuali impatti.

7. Sanzioni disciplinari

Le informazioni identificate durante eventuali controlli possono essere utilizzate e conservate per la durata di ogni procedimento investigativo, disciplinare o regolamentare e possono essere comunicate a terze parti (es. avvocati) quando necessario.
In particolare, l'azienda, in ottica di quanto precedentemente definito, nel caso constati che la posta elettronica e/o la rete Internet sono utilizzate indebitamente, può intervenire disciplinarmente nei confronti dell'Utente riconosciuto responsabile applicando il sistema sanzionatorio in vigore.
Rimane salva la denuncia all'autorità competente qualora il comportamento costituisca reato.

8. Ruoli e responsabilità

Nel seguente paragrafo vengono riportati i principali ruoli e le relative responsabilità che svolgono una funzione chiave nel garantire il coretto utilizzo degli strumenti informatici aziendali e del loro funzionamento.

8.1 HRBP

Gli HRBP sono responsabili di:

- supportare le strutture aziendali di competenza nella definizione, revisione e aggiornamento dei requisiti di sicurezza inclusi nel presente Regolamento;
- assicurarsi che i requisiti definiti nel presente Regolamento siano divulgati in maniera appropriata e portati a conoscenza dei dipendenti e delle terze parti;
- definire e intraprendere i procedimenti disciplinari previsti nei confronti degli individui per i quali sia stata verificata una violazione dei principi del presente Regolamento.

8.2 Legal Affairs

Legal Affairs, per lo scopo di questo regolamento, è responsabile di:

- supportare le strutture aziendali di competenza durante la definizione, la revisione e l'aggiornamento dei requisiti di protezione inclusi all'interno di questo regolamento e di garantire che sia conforme alle leggi e alle normative applicabili;
- garantire che le investigazioni siano condotte in conformità con le leggi e i regolamenti applicabili;

- promuovere azioni legali nei confronti di persone o entità coinvolte in una violazione del presente regolamento.

8.3 Organization

Organization è responsabile delle seguenti mansioni:

- supportare le strutture aziendali di competenza nella definizione, revisione e aggiornamento dei requisiti di sicurezza inclusi nel presente Regolamento;
- supportare e /o gestire eventuali anomalie, problemi o incidenti legati all'ambito GDPR.

8.4 ICT Governance, Integration & Security

ICT Governance, Integration & Security è responsabile di:

- definire, revisionare e aggiornare i requisiti di sicurezza inclusi nel presente Regolamento;
- supportare la UO ICT nell'identificazione delle soluzioni tecniche e organizzative messe in atto per soddisfare i requisiti inclusi nel presente Regolamento;
- gestire ogni violazione del presente Regolamento.

8.5 Responsabili di Unità Organizzativa

I Responsabili di Unità Organizzativa sono incaricati di:

- garantire che le norme all'interno di questo Regolamento siano state rispettate dei soggetti sottoposti alla loro responsabilità;
- comunicare alle strutture aziendali di competenza qualsiasi violazione dei requisiti di cui all'interno di questo Regolamento.

8.6 Utente

Per "utente" si intende qualunque persona fisica (es. dipendente, collaboratore, stagista fornitore ecc.) che utilizzi gli strumenti informatici aziendali.
Pertanto, l'utente:

- è personalmente responsabile dell'utilizzo degli strumenti informatici che gli vengono affidati dall'azienda nonché dei relativi dati trattati per finalità aziendali;
- è tenuto a tutelare (per quanto di propria competenza) il patrimonio aziendale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia;
- è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno.