

REG. n. 30

REGOLAMENTO INFORMATICO

Norme per il corretto utilizzo degli strumenti informatici e dei dati aziendali

Indice

1.	PREMESSA	3
2.	AMBITO DI APPLICAZIONE DELLE NORME	4
3.	CRITERI GENERALI	4
4.	CONTROLLI PER GARANTIRE LA SICUREZZA DELL'INFRASTRUTTURA INFORMATICA	5
4.1	Sistemi di controllo graduati.....	5
4.2	Registrazione degli accessi.....	6
5.	RESPONSABILITÀ DEGLI UTENTI DEI SISTEMI INFORMATIVI	6
6.	CONSEGUENZE NEL CASO DI VIOLAZIONI E SANZIONI	7
7.	DIFFUSIONE DELLE NORME PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI	7
8.	NORME DI UTILIZZO DEI DISPOSITIVI INFORMATICI	7
8.1	Cura materiale dei dispositivi aziendali personali	8
8.2	Utilizzo corretto dei dispositivi aziendali	8
8.3	Proibizioni ad effettuare modifiche fisiche al dispositivo	9
8.4	Modifica della configurazione dei computer aziendali	9
8.5	Utilizzo di computer non aziendali in rete aziendale (BYOD).....	10
8.6	Richiesta di assistenza	11
8.7	Segnalazioni di guasti, anomalie o violazioni della sicurezza	11
9.	GESTIONE DELLE CREDENZIALI PERSONALI.....	11
9.1	Rilascio delle credenziali personali.....	11
9.2	Il processo di concessione di autorizzazioni e privilegi	12
9.3	Gestione delle credenziali.....	12
9.4	La revoca delle credenziali	13
10.	PROTEZIONE DEI DATI NEI DISPOSITIVI e NEI SUPPORTI RIMOVIBILI.....	13
10.1	Dove memorizzare i dati di interesse aziendale, personali o riservati utilizzati per scopi lavorativi.....	14
10.2	Proibizione all'utilizzo di dati estranei alle attività lavorative	14
10.3	Misure di protezione di dati su supporti cartacei.....	15
10.4	Condivisioni dei dati.....	15
11.	NORME DI UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE	15
11.1	Contenuti dei messaggi di posta elettronica.....	15
11.2	Finalità di utilizzo dei messaggi di posta elettronica.....	17
11.3	Accesso al sistema di posta elettronica	18
11.4	Firma dei messaggi di posta elettronica	18
11.5	Protezione contro i virus, malware e spam nell'ambito del sistema di posta elettronica	19
12.	NORME DI UTILIZZO INTERNET	20
12.1	Accesso ad Internet.....	20
12.2	Download di software	21
13.	PROTEZIONE ANTIVIRUS E ANTI-MALWARE	21
14.	UTILIZZO DEI TELEFONI, FAX E FOTOCOPIRIFICI AZIENDALI	22
15.	NORME SPECIFICHE PER TELELAVORO E SMART WORKING	22
16.	AGGIORNAMENTO E REVISIONE	24

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, in particolare, il libero accesso alla rete Internet dai Personal Computer aziendali, e l'uso degli strumenti informatici aziendali espongono Etra S.p.A. - e le Società del Gruppo che utilizzano in service parte del patrimonio informativo della controllante - a rischi di natura patrimoniale, oltre che a responsabilità penali conseguenti la violazione di specifiche disposizioni di legge (fra tutte, legge sul diritto d'autore e legge sulla privacy), con conseguenti ripercussioni sulla sicurezza e sull'immagine dell'Azienda stessa.

Per strumenti informatici s'intende l'insieme delle risorse informatiche di Etra S.p.A., ovvero le risorse infrastrutturali e del patrimonio informativo digitale. Le risorse infrastrutturali sono costituite dalle componenti hardware e software, mentre il patrimonio informativo è l'insieme delle banche dati in formato digitale, nonché di tutti i documenti, anche cartacei, prodotti tramite l'utilizzo delle risorse infrastrutturali o comunque disponibili nelle sedi aziendali.

Il lavoratore è responsabile della propria prestazione di lavoro e deve custodire ed utilizzare gli strumenti informatici, le risorse infrastrutturali, il patrimonio informativo e la posta elettronica in modo appropriato all'attività lavorativa svolta, secondo i principi di diligenza e correttezza nel pieno rispetto del codice etico aziendale.

Per evitare che comportamenti, anche inconsapevoli, dei lavoratori possano minacciare e/o compromettere la sicurezza nel trattamento dei dati, ovvero comportamenti scorretti distolgano le risorse aziendali dall'uso cui le stesse sono deputate, Etra S.p.A. definisce le regole per una *policy* sulla sicurezza delle informazioni in Azienda e per la corretta gestione dei sistemi informatici e adotta il presente Regolamento.

Ogni utente dei sistemi informativi è tenuto al rispetto delle norme comportamentali e degli standard definiti nel presente documento, nell'utilizzo dei dispositivi Informatici assegnatigli e nella gestione dei dati aziendali di propria competenza.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per utente deve intendersi ogni dipendente, senza distinzione di ruolo e/o livello, collaboratore, a prescindere dal rapporto contrattuale intrattenuto con l'Azienda (collaboratore a progetto, in stage, consulente, ecc.) o qualunque persona che rivesta cariche per l'azienda, in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "Autorizzato al trattamento" in virtù dell'autorizzazione al trattamento già assegnata ai sensi dell'art. 29 del Reg. UE 679/2016 (cd. GDPR).

Le prescrizioni di seguito previste, infatti, si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli Autorizzati al trattamento, in attuazione del D.Lgs. 30 giugno 2003 n. 196 e ss.mm.ii. e del Reg. UE 679/2016 riportando, altresì, le informazioni già fornite in ordine alle ragioni, alle modalità dei possibili controlli e alle conseguenze sanzionatorie -in caso di violazione

delle stesse. Inoltre, il presente Regolamento contempla i doveri e le modalità che ciascun collaboratore deve osservare nell'utilizzo di specifici apparecchi elettronici, come telefoni e altri mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), che Etra S.p.A., nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte.

Le **sanzioni** applicabili in caso di mancato rispetto del presente regolamento e delle istruzioni fornite da Etra possono essere di varia natura, compresa quella risarcitoria, a seconda del rapporto giuridico esistente tra la società e l'utente. A titolo esemplificativo e non esaustivo, le sanzioni possono essere di tipo disciplinare, risarcitorio, di revoca d'incarichi e risoluzioni contrattuali.

2. AMBITO DI APPLICAZIONE DELLE NORME

Questo documento descrive le norme comportamentali e le linee guida per il corretto utilizzo che l'utente deve seguire quando utilizza strumenti aziendali informatici quali, a titolo indicativo e non esaustivo:

- ☐ Desktop, Notebook e accessori forniti dall'Azienda;
- ☐ Tablet, Smartphone, SIM voce e SIM dati forniti dall'Azienda;
- ☐ Dispositivi di memorizzazione removibili forniti dall'Azienda;
- ☐ Dispositivi di uso comune quali: apparati di videoconferenza, audioconferenza, fotocopiatrici, ecc.
- ☐ Credenziali personali di accesso al dominio ed alle sue risorse;
- ☐ Risorse del Sistema Informatico Aziendale;
- ☐ Posta elettronica aziendale;
- ☐ Accesso ad Internet;
- ☐ Accesso remoto alla rete aziendale.

Il presente regolamento entrerà in vigore il 01/07/2023. Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, verrà reso disponibile a ciascun utente attraverso il "Portale del Dipendente" ed nella Pagina Intranet aziendale".

3. CRITERI GENERALI

I rischi che possono derivare da una non corretta utilizzazione delle risorse informatiche sono innescati da attività malevole esogene all'Azienda (malware, virus, ransomware, ecc.) o da comportamenti volontari o involontari degli utenti. Pertanto, è necessario che il comportamento degli utenti sia:

- ☐ competente nel conoscere i possibili effetti di una attività informatica;
- ☐ prudente nel valutare sempre le possibili conseguenze di ogni azione;

- ☐ diligente nel rispettare sempre le norme qui esposte.

Tale disciplina ha lo scopo di salvaguardare e difendere il patrimonio aziendale, nel pieno rispetto delle norme di tutela dei lavoratori, escludendo quindi ogni utilizzo che realizzi “controllo a distanza” o “indagine sulle opinioni” (profilazione). Il criterio generale che l'utente deve seguire è quello di evitare che le attività svolte possano:

- ☐ produrre danni economici e patrimoniali all'Azienda per la perdita di beni materiali o immateriali o per l'impossibilità di rispettare i contratti con i Clienti o Fornitori a causa di blocchi informatici o perdite di dati;
- ☐ costituire un rischio per la sicurezza dei dati propri, di altre persone, dell'Azienda o di Clienti o Fornitori verso i quali l'Azienda assuma una responsabilità in relazione al loro trattamento e che possano andare distrutti, non correttamente trattati o divulgati a terzi non autorizzati;
- ☐ essere contrarie all'etica aziendale ed ai principi che regolano il corretto rapporto di lavoro;
- ☐ procurare danni di immagine all'Azienda;
- ☐ configurarsi in generale come reati per la normativa vigente.

4. CONTROLLI PER GARANTIRE LA SICUREZZA DELL'INFRASTRUTTURA INFORMATICA

Per le ragioni esposte nel paragrafo precedente, è facoltà della Società, con l'ausilio del Personale dell'Unità Organizzativa Servizi Informativi (d'ora in poi, per brevità ICT) o di gestori esterni - rispettivamente nominati Autorizzati al Trattamento ex art. 29 GDPR o Responsabili Esterni ai sensi dell'art. 28 GDPR - accedere a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico per effettuare dei controlli con l'obiettivo di verificare l'insorgenza di eventuali minacce alla sicurezza dell'infrastruttura dell'Azienda, nonché per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione di costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc). Tali controlli, che possono avvenire occasionalmente e senza preavviso, sono svolti in conformità a quanto stabilito dall'art. 4 dello Statuto dei Lavoratori (L. 300/1970 e ss.mm.ii.) e dalla vigente normativa sul trattamento dei dati personali.

Nel caso in cui, a seguito dei controlli effettuati, si riscontri una violazione alle norme descritte nel presente documento, la Società provvede alle opportune verifiche e valuta la necessità di applicare eventuali sanzioni nonché di informare le Autorità competenti.

4.1 Sistemi di controllo graduati

In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si

inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Resta fermo in ogni caso l'obbligo per il personale incaricato del Servizio ICT di effettuare i controlli strettamente necessari a garantire la sicurezza e la salvaguardia del sistema informatico.

4.2. Registrazione degli accessi

Al fine di poter identificare l'accesso fraudolento o l'uso abusivo di dati personali, o per determinare l'origine di un incidente, è necessario registrare determinate azioni eseguite sui sistemi IT. Tali registri sono conservati per un periodo non superiore ai 180 giorni, tranne nel caso di obbligo legale o di un rischio particolarmente significativo per i diritti e le libertà degli interessati.

I registri sono configurati per registrare le anomalie e gli eventi relativi alla sicurezza. Gli accessi devono essere registrati con il loro identificatore, la data e l'ora della loro connessione, così come la data e l'ora della loro disconnessione.

Tali registri si trovano all'interno di ciascun strumento di lavoro e vengono attivati soltanto per le finalità di tutela dei dati personali trattati. I dati rilevati dai registri non potranno essere utilizzati per finalità di controllo dei lavoratori/utenti e per finalità disciplinari.

L'accesso ai file di registro è consentito al personale del Servizio ICT, per verificare eventuali anomalie nelle registrazioni. L'accesso è altresì consentito in caso di data breach al fine di verificare le modalità dell'incidente.

5. RESPONSABILITÀ DEGLI UTENTI DEI SISTEMI INFORMATIVI

Ciascun utente dei sistemi informativi è responsabile della sicurezza ICT. Ognuno è pertanto tenuto al corretto utilizzo dei dispositivi informatici assegnatogli, secondo le modalità previste dalle singole applicazioni e nel rispetto degli standard di sicurezza enunciati nel presente documento, riguardanti l'integrità e l'affidabilità dei dati aziendali e personali.

I dispositivi informatici ed i pacchetti software sono assegnati in dotazione all'utente esclusivamente per lo svolgimento delle proprie mansioni aziendali.

Ognuno è altresì tenuto a:

- ☐ segnalare guasti all'attrezzatura informatica e di telefonia in dotazione;
- ☐ segnalare malfunzionamenti delle applicazioni e del software di base;
- ☐ segnalare anomalie nei dati gestiti.

Per le richieste di approvvigionamento o acquisto di materiale hardware, software, telefonia, ciascun utente deve rivolgersi al proprio Responsabile di Funzione, il quale si occuperà di inoltrare la richiesta all'Assistenza IT.

Ogni utente dell'azienda, come sopra definito, senza distinzione di ruolo e/o livello è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi a cui hanno accesso e ai dati trattati ai fini aziendali. Gli utenti sono altresì responsabili del contenuto delle comunicazioni effettuate e ricevute ai fini aziendali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui comunicazione e diffusione impropria potrebbe configurare violazione della normativa per la tutela dei dati personali. Sono inoltre vietati comportamenti che possono creare un danno, anche di immagine, all'azienda. È obbligatorio per ogni utente, nonché per il personale del Servizio ICT, attenersi alle disposizioni vigenti in materia di Protezione dei dati personali.

6. CONSEGUENZE NEL CASO DI VIOLAZIONI E SANZIONI

Tutti gli utenti, come sopra definiti, sono obbligati ad osservare e rispettare le norme indicate nel presente documento. Nel caso di violazione volontaria o involontaria di queste norme, l'Azienda può anche stabilire, in base alla gravità del fatto in sé o delle conseguenze che esso ha comportato, di procedere nei confronti dell'utente con l'applicazione di specifici provvedimenti disciplinari e/o di tutte le azioni civili e penali consentite, comprese eventuali azioni risarcitorie. Tali provvedimenti saranno applicati nel rispetto della procedura disciplinare stabilita dal CCNL Gas-Acqua, dal CCNL Federambiente, dal CCNL Confservizi Dirigenti, dal Modello Organizzativo di gestione e controllo di Etra (D.Lgs. 231/01 e ss.mm.ii.) dal Codice Etico, dal codice di comportamento e dallo Statuto dei Lavoratori, ove applicabili.

Qualora la violazione sia effettuata attraverso la disponibilità di permessi di amministrazione del proprio computer, tale permesso verrà revocato d'ufficio dal Servizio ICT.

7. DIFFUSIONE DELLE NORME PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI

Ogni Responsabile di Area/Funzione avrà cura nel favorire ed assicurare la diffusione delle presenti norme a tutti i componenti dell'Unità Organizzativa dallo stesso coordinata, a tutti i livelli ed in particolar modo nel momento in cui vi siano nuovi ingressi e nuove assunzioni.

8. NORME DI UTILIZZO DEI DISPOSITIVI INFORMATICI

Il Personal Computer (PC) affidato all'utente, così come lo Smartphone e il Tablet, è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Tali dispositivi devono essere custoditi con cura evitando ogni possibile forma di danneggiamento.

8.1 Cura materiale dei dispositivi aziendali personali

Ogni utilizzatore dei dispositivi informatici aziendali è responsabile della sicurezza materiale degli stessi. A tal riguardo, tutti gli utenti sono tenuti al rispetto delle seguenti regole:

- ☐ durante le trasferte non lasciare il dispositivo personale in aree pubbliche, ancorché chiuso all'interno della vettura, tal che possa essere facilmente oggetto di furto. Il furto del dispositivo ha una doppia conseguenza: un danno economico per l'Azienda e la possibilità di perdita di dati personali propri o di terzi contenuti nel dispositivo. È pertanto opportuno portare con sé il dispositivo in ogni evenienza, nonché adottare adeguati criteri di protezione dei dati di cui al paragrafo relativo. Nel caso di trasporto su veicoli e in tutti i casi di sosta temporanea in cui non sia possibile portare con sé il dispositivo personale, è necessario riporre il materiale nel bagagliaio assicurandosi sempre che i cristalli del veicolo siano rialzati e le portiere chiuse a chiave;
- ☐ in caso di furto/smarrimento del dispositivo è necessario effettuare tempestiva denuncia alle Autorità Competenti, informando senza ingiustificato ritardo la Società e i Servizi ICT;
- ☐ non utilizzare il dispositivo in modo improprio in modo che sia messo a rischio di guasto o che sia danneggiato per effetto di urti, liquidi, polvere, fonti di calore eccessive o altri agenti esterni;
- ☐ nel caso si renda necessario inviare il dispositivo in altra sede con qualunque mezzo, l'utente assegnatario si deve accertare che l'imballaggio per il trasporto sia adeguato a proteggere il dispositivo da urti o danneggiamenti;
- ☐ spegnere, al termine del proprio lavoro e comunque alla fine della giornata lavorativa, il proprio computer e tutte le macchine attive nella propria postazione di lavoro (come ad esempio stampanti locali, calcolatrici, ecc.) in modo da non lasciare dei dispositivi accesi senza un adeguato presidio e al fine, inoltre, di ridurre il consumo di energia quando non utilizzati;
- ☐ riporre in luoghi sicuri i computer portatili, i dispositivi rimovibili e i documenti cartacei una volta fuori dall'ufficio.

8.2 Utilizzo corretto dei dispositivi aziendali

Salvo casi particolari, che vanno specificatamente segnalati alla Direzione e al Servizio ICT, che ne terrà conto nei propri controlli, l'uso del dispositivo personale aziendale è riservato esclusivamente all'utente assegnatario. È quindi vietato concederne l'utilizzo a terzi.

L'utilizzo del computer aziendale e degli altri dispositivi informatici personali è destinato ai soli scopi lavorativi. Quindi ne è vietato l'uso a titolo personale, installando programmi che non hanno alcun rilievo lavorativo o depositando nel computer propri dati personali.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete di Etra S.p.A. solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo paragrafo 9 del presente Regolamento.



È assolutamente vietato installare o semplicemente ospitare programmi illeciti o pericolosi o considerati tali utilizzati per lo più per attività di "hacking" o di "cracking".

È assolutamente vietato detenere software e file multimediali che violano i diritti di autore (film, musica, fotocopie di testi, ecc.).

È assolutamente vietato utilizzare il computer, il telefono cellulare, smartphone o tablet per azioni contro l'etica, la morale e in violazione alle leggi vigenti.

Non utilizzare il computer per accedere alla propria posta privata non aziendale. La posta privata potrebbe non essere protetta dal virus e malware come quella aziendale. Aprire allegati di posta senza tale controllo potrebbe costituire una seria minaccia alla sicurezza del computer e dell'intero sistema e causare gravi danni.

Non è consentito dal computer accedere a siti Web per motivi estranei alla propria attività lavorativa, se non in modo del tutto episodico e straordinario e fuori dall'orario di lavoro.

8.3 Proibizioni ad effettuare modifiche fisiche al dispositivo



È assolutamente vietato manomettere o modificare o smontare il dispositivo per rimuovere o sostituire parti. Non tentare di ripararlo in caso di guasto. In tali evenienze affidarsi esclusivamente al Servizio ICT.

Non applicare adesivi o rimuovere quelli esistenti (matricola dispositivo, licenza software OEM, ecc..) o segnare o incidere indelebilmente la superficie del dispositivo.

8.4 Modifica della configurazione dei computer aziendali

Il computer e tutti i dispositivi mobili (quali smartphone e tablet) vengono consegnati con tutte le dotazioni necessarie a garantire il funzionamento e ad assicurare un criterio di sicurezza di base. L'Utente, indipendentemente dal tipo di sistema operativo e dai permessi che gli sono stati concessi, non può di regola effettuare determinate modifiche alla loro configurazione, né effettuare l'installazione di programmi o di dispositivi di memorizzazione, comunicazione o altro diversi da quelli ufficialmente installati dal personale del Servizio ICT per conto di Etra S.p.A. (masterizzatori, modem, etc.). Ciò deve essere giustificato esclusivamente per motivi di lavoro, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L'inosservanza della presente disposizione espone la stessa Etra S.p.A. a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziati, o comunque liberi e quindi non protetti dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico di Etra S.p.A., come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, con conseguente applicazione di sanzioni pecuniarie ed interdittive.

Nel caso necessitano tali modifiche senza averne il permesso l'utente può, su richiesta del proprio Responsabile di Funzione, affidarsi al Servizio ICT che può operare sul dispositivo e farsi

concedere, temporaneamente o permanentemente, i permessi di cui necessita per effettuare tali modifiche.

Ogni maggiore libertà di intervento concessa all'utente deve essere sempre controbilanciata da:

- ☐ accortezza e prudenza nell'evitare di aprire varchi a minacce alla sicurezza o nel procurare danni;
- ☐ consapevolezza nel non compiere azioni contrarie all'etica aziendale e alle leggi vigenti.

La violazione di queste norme può comportare la revoca immediata di tali permessi, pertanto:



- ☐ non caricare o installare programmi non precedentemente autorizzati da ICT. La detenzione di software privo di regolare licenza e reso operativo con particolari accorgimenti (programmi "craccati") costituisce un reato;
- ☐ nel caso si disponga delle credenziali di amministrazione del computer personale è comunque assolutamente vietato alterarne la configurazione standard, in quanto ciò può provocare una grave vulnerabilità di fronte ad attacchi esterni. In particolare, è vietato:
 - modificare il dominio originario;
 - cambiare la configurazione dell'IP e del Proxy;
 - rimuovere o disabilitare i sistemi di sicurezza (ad es. antivirus);
 - creare altri amministratori della macchina o altri utenti locali
- ☐ non rimuovere l'automatismo di messa in standby del computer dopo DIECI minuti di inattività (screen saver). Nel caso il computer utilizzato non sia dotato di questo automatismo;
- ☐ non modificare le "group policy" locali;
- ☐ non attivare sistemi di connessione alternativi e non protetti (ad es. modem del telefono in *tethering*) mentre si è collegati in rete aziendale (*wired o wireless*).

8.5 Utilizzo di computer non aziendali in rete aziendale (BYOD)

Con il termine generico di BYOD (*Bring Your Own Device*) o "Dispositivo terzo" nel contesto di questo documento si intende un dispositivo di utilizzo personale (notebook, smartphone, tablet, USB storage) non fornito o controllato dall'Azienda, ma ospitato all'interno della rete aziendale.

Agli utenti ai quali venga fornito un computer dell'azienda non è consentito in alcun modo l'utilizzo di dispositivi BYOD se non in casi eccezionali, su espressa autorizzazione del servizio ICT.

L'Utente, per utilizzare il proprio dispositivo in rete Aziendale, deve:

- ☐ consentire al Servizio ICT di accedere preventivamente e periodicamente al dispositivo BYOD per verificare lo stato degli strumenti di sicurezza installati (antivirus, aggiornamento S.O., presenza di software sospetto o non licenziato);

- accettare che il Servizio ICT installi eventuali software di protezione anti-malware o agent per il collegamento con il centro di controllo.

8.6 Richiesta di assistenza

L'assistenza da parte del personale del Servizio ICT incaricato ed autorizzato ad effettuare gli interventi di cui possa sorgere necessità viene richiesta ed autorizzata esclusivamente dal Responsabile di Area/Funzione di riferimento dell'utente, attraverso strumenti specifici messi a disposizione da ICT. In caso di oggettiva necessità, o a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico, l'intervento da parte del personale del Servizio ICT potrà essere eseguito anche in assenza di una specifica richiesta dovrà immediatamente ed obbligatoriamente contattare il Responsabile di Area/Funzione il quale autorizzerà l'intervento sul sistema informatico e telematico.

Tutti gli altri utenti richiederanno direttamente l'intervento del personale del servizio ICT attraverso gli strumenti specifici messi a disposizione da ICT.

Nelle richieste di intervento è sempre necessario che vengano espone compiutamente la questione e/o la richiesta.

8.7 Segnalazioni di guasti, anomalie o violazioni della sicurezza

Ogni guasto fisico o ogni anomalia funzionale dei dispositivi devono essere segnalati al Servizio ICT.

L'Utente è inoltre responsabile della tempestiva segnalazione di attacchi di virus o malware, di violazioni alla sicurezza o alla privacy potenziali o in atto e di ogni altra concomitanza od evento contrarie ai principi ed alle norme qui indicate al fine di permettere al Personale del Servizio ICT di poter prontamente intervenire e mettere in atto tutte le procedure per l'eventuale notifica del Data Breach all'Autorità Garante secondo le istruzioni operative adottate dalla Società.

9. GESTIONE DELLE CREDENZIALI PERSONALI

9.1 Rilascio delle credenziali personali

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, che ne darà comunicazione al Responsabile di Area/Funzione -previa comunicazione da parte di HR dell'inserimento della nuova risorsa- il Responsabile di Area/Funzione provvederà a fornire al personale dei servizi ICT l'elenco degli applicativi e dei collegamenti d'abbinare al nuovo profilo tenendo conto dell'ambito nel quale verrà inserita la nuova risorsa. Nel caso di collaboratori a progetto e coordinati e continuativi, la preventiva richiesta, se necessaria, verrà inoltrata dal Responsabile di Area/Funzione con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (*user id*), assegnato dal Servizio ICT, associato ad una parola chiave (*password*) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non dovrà essere divulgata. Non è consentita l'attivazione della password di accensione (*bios*), senza preventiva autorizzazione da parte del Servizio ICT.

È necessario procedere alla modifica della parola chiave a cura dell'utente, autorizzato al trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.

Le credenziali di accesso aziendali consentono di accedere:

- ☐ al proprio device;
- ☐ al sistema informatico aziendale (es. server);
- ☐ ai software, ai database, ai portali e ai gestionali utilizzati per il proprio lavoro direttamente collegati al sistema di autenticazione aziendale alla propria casella di posta.

9.2 Il processo di concessione di autorizzazioni e privilegi

L'accesso degli utenti al sistema aziendale è regolato dalle abilitazioni specifiche nel rispetto del trattamento dei dati nell'area organizzativa di riferimento.

Qualora sia necessario per motivi di lavoro, l'utente può richiedere al proprio Responsabile di Funzione di:

- ☐ accedere a cartelle riservate ad altri utenti o gruppi di lavoro;
- ☐ accedere da remoto via VPN al sistema;
- ☐ disporre (temporaneamente o permanentemente) dei permessi di amministrazione del proprio computer.

Tali richieste devono essere effettuate dal Responsabile di Funzione, il quale le trasmetterà al Servizio ICT.

9.3 Gestione delle credenziali

Le credenziali sono personali e chiunque le fornisca a terzi per qualsiasi motivo incorre in una grave violazione dei criteri di sicurezza.

Le password sono controllate in modo che presentino obbligatoriamente le seguenti caratteristiche:

- ☐ siano composte da almeno 8 caratteri;
- ☐ siano diverse dalle precedenti 3 password;
- ☐ siano variate ogni 90 giorni;
- ☐ siano bloccate dopo 15 tentativi errati.

Oltre a ciò, è opportuno che le password abbiano delle caratteristiche tali che ne impediscano una facile identificazione:

- ☐ non utilizzare una password che sia uguale all'identificativo utente, né al proprio nome e cognome;
- ☐ non utilizzare una password che sia facilmente intuibile o ripetitiva;
- ☐ evitare di scegliere parole comunemente usate, quali nomi propri o di località, nome dell'azienda o simili in quanto possono facilmente essere identificabili dai programmi hacker;
- ☐ evitare di scegliere parole agevolmente riconducibili all'utente;
- ☐ evitare parole contenute nelle password precedenti.

È consigliabile ricordare le proprie password a memoria evitando di scriverle su carta o nel computer o comunque dove possano essere lette da terzi. Nel caso di dimenticanza è sempre possibile rivolgersi al Servizio ICT che può resettare le password in modo che l'utente possa inserirne di nuove.

Cambiare immediatamente le password se si ha il sospetto che la stesse abbiano perso la necessaria segretezza.

Non utilizzare le proprie credenziali, né il proprio indirizzo di posta elettronica, per iscriversi a newsletter, mailing list o per registrarsi su siti estranei alle attività lavorative.

9.4 La revoca delle credenziali

L'accesso ai sistemi informatici aziendali di un utente che chiude il rapporto contrattuale con l'azienda viene disabilitato su comunicazione al Personale del Servizio ICT da parte dell'Ufficio Risorse Umane, nell'immediatezza della cessazione del rapporto lavorativo. Eventuali deroghe a quanto sopra, giustificate da particolari ragioni di opportunità aziendali, dovranno essere autorizzate dalla Società.

10. PROTEZIONE DEI DATI NEI DISPOSITIVI e NEI SUPPORTI RIMOVIBILI

Le norme seguenti si applicano a computer (portatili o fissi) e ai supporti di archiviazione di massa removibili (chiavette USB, hard disk USB) nonché a smartphone e tablet.

Con il termine generico di "dati" si indicano in questo paragrafo e nei successivi le seguenti categorie:

- ☐ dati di interesse aziendale personali o riservati utilizzati per scopi lavorativi;
- ☐ dati strettamente personali ma utilizzati in ambito lavorativo;
- ☐ dati estranei alle attività lavorative quali contenuti multimediali (film, musiche digitali, foto personali), software ecc. detenuti o meno in violazione alle leggi sui diritti d'autore.

Tutti i supporti magnetici removibili aziendali, preventivamente autorizzati, (es.: dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali, nonché informazioni costituenti know-how

aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili, ciascun utente dovrà riconsegnarli al Servizio ICT.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

10.1 Dove memorizzare i dati di interesse aziendale, personali o riservati utilizzati per scopi lavorativi

L'utente è responsabile del corretto utilizzo dei dati trattati a cui ha accesso.



La memorizzazione dei suddetti dati non deve mai trovare luogo, se non in casi eccezionali, sui dischi fissi dei dispositivi personali o su dispositivi rimovibili quali hard disk esterni o chiavette USB o in aree comuni (ad es. sui PC delle sale di videoconferenza).

Per la memorizzazione di tali dati si devono utilizzare aree dedicate all'interno del sistema informatico aziendale (es. server), accessibili solo al personale che ne ha titolo, che sono sottoposte a backup giornaliero e che possono essere create/attivate dietro specifica richiesta del Responsabile di Funzione/Area al Servizio ICT per un gruppo di lavoro o anche per un singolo utente.

Nei casi in cui sia necessario, ad esempio per ragioni di efficienza operativa, depositare queste tipologie di dati sui dischi fissi dei dispositivi in dotazione o su dispositivi rimovibili quali hard disk esterni o chiavette USB o in aree comuni, verificare che essi siano:

- ☒ duplicati per sicurezza su cartelle condivise;
- ☒ crittografati durante gli eventuali trasferimenti del dispositivo all'esterno;
- ☐ conservati in armadi o cassetti chiusi al di fuori delle ore di ufficio o in assenza della custodia dell'autorizzato;
- ☐ rimossi da tali supporti immediatamente dopo il loro utilizzo.

Il trattamento dei dati riferiti alle persone fisiche deve inoltre ottemperare al Regolamento Europeo 679/2016 (GDPR) che l'Azienda ha recepito e formalizzato nei presenti documenti. Durante il trattamento di dati personali fare riferimento all'U.O. Sistema Gestione Integrato e Privacy per ogni dubbio e chiarimento.

10.2 Proibizione all'utilizzo di dati estranei alle attività lavorative



Non è assolutamente consentito memorizzare dati estranei al proprio lavoro quali: film, musiche in formato digitale, foto digitali, software ecc. ovvero password personali, pin del proprio bancomat o della propria carta di credito ecc.

Costituisce una grave violazione il detenere su supporti e dispositivi aziendali materiale illegale per contenuti o perché in violazione alle norme sui diritti d'autore.

10.3 Misure di protezione di dati su supporti cartacei

L'utente è responsabile della custodia dei supporti cartacei e dei dati aziendali o personali in essi contenuti.

I documenti cartacei contenenti informazioni aziendali riservate o dati personali devono essere prontamente rimossi dai luoghi comuni, quali fotocopiatrici o stampanti di corridoio, a cura dell'autorizzato.

In modo analogo, al di fuori delle ore d'ufficio o in assenza della sorveglianza degli autorizzati, tali documenti devono essere conservati in armadi o cassetti chiusi a chiave e le scrivanie devono essere sgombrare (*clean desk policy*). I singoli uffici, inoltre, devono essere chiusi a chiave.

10.4 Condivisioni dei dati

I dati aziendali trattati ai fini di lavoro devono essere condivisi fra gruppi di lavoro tramite aree dell'infrastruttura informatica accessibili esclusivamente a chi ne ha diritto.



È assolutamente vietato comunicare ai colleghi dipendenti, collaboratori o terzi non specificatamente incaricati od autorizzati a trattarle, informazioni aziendali riservate, dati personali di nessuna natura che fossero stati acquisiti durante l'esercizio del proprio compito lavorativo.

11. NORME DI UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

Le politiche sull'uso della posta elettronica riguardano tutti gli utenti dei sistemi informativi aziendali, interni ed esterni, compresi quindi gli utilizzatori occasionali, quali consulenti, fornitori e agenti. Queste politiche vanno applicate al personale che lavora su dispositivi informatici resi disponibili dall'azienda, che siano o no di proprietà, che siano o no situate nei locali della stessa azienda. Inoltre, queste politiche si applicano alle comunicazioni provenienti da tutti gli apparecchi elettronici, compresi, senza alcun limite, personal computer, computer portatili, dispositivi di assistenza digitali (ad esempio, dispositivi senza filo come "palmari" bluetooth o Wireless) e cellulari.

11.1 Contenuti dei messaggi di posta elettronica

Tutti i messaggi aziendali presenti nel Sistema di Posta Elettronica devono essere formulati in modo professionale e devono poter essere visionati senza creare imbarazzo all'Azienda e ai suoi dipendenti, clienti o fornitori.

Tutti i messaggi inviati dal sistema di posta devono essere compatibili con le politiche dell'Azienda e le pratiche di condotta morale, sicurezza, conformità alle leggi applicabili e alle pratiche commerciali, nonché alle disposizioni impartite dalla Direzione.

Tutte le politiche aziendali, comprese, senza alcuna limitazione, quelle relative ai diritti d'autore, alla riservatezza, alla discriminazione, alle molestie e al rispetto delle leggi sull'equo impiego, sono applicate all'uso della posta elettronica e ai Sistemi di Posta.

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro il cui utilizzo per fini personali non è consentito come meglio specificato in seguito.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica con dominio aziendale (n.cognome@etraspa.it) per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- ☐ l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali non legati all'attività lavorativa;
- ☐ l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- ☐ la partecipazione a catene telematiche. Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Etra S.p.A. ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile di Area/Funzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di Area/Funzione, a seconda del loro contenuto e dei destinatari delle stesse.

È obbligatorio porre la massima attenzione nell'aprire i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti).

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) potrà inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere preventivamente attivata dall'utente.

In caso di assenza non programmata (ad es. per malattia) la procedura dovrà essere attivata, entro due giorni, attraverso il servizio web mail messo a disposizione; in caso di impossibilità, verrà attivata a cura dell'azienda.

Sarà comunque consentito al superiore gerarchico dell'utente, al verificarsi delle situazioni di sicurezza ed urgenza sopra indicate, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: a causa della mancata attivazione della funzionalità di risposta automatica).

Il personale del servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà resettare, previa autorizzazione da parte del Responsabile di Area/Funzione la password d'accesso alla casella di posta elettronica affinché lo stesso Responsabile di Area/Funzione possa svolgere le operazioni strettamente necessarie a garantire la sicurezza e la salvaguardia del sistema informatico.

Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato di Etra S.p.A. potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

Inoltre, è severamente vietato:



- ☐ l'invio di informazioni commerciali e dati riservati, o esclusivi, o segreti, a persone estranee non autorizzate a riceverle, sia all'interno che all'esterno dell'Azienda;
- ☐ l'invio di materiali o link proibiti o limitati da regolamenti sulla sicurezza;
- ☐ la distribuzione o l'invio di materiali protetti dal diritto d'autore tramite i sistemi di posta elettronica o altri mezzi, in violazione delle leggi sui diritti d'autore o sui contratti di licenza;
- ☐ l'invio di messaggi con contenuti che possano essere considerati discriminatori, osceni, umilianti o eccessivamente personali, sia seri che umoristici o interpretati come molestie sessuali. I messaggi di posta elettronica possono essere considerati diffamatori nei confronti di terzi ed è pertanto fatto divieto di esprimere critiche personali o commenti polemici o calunniosi o offensivi nei confronti di colleghi, Clienti o Fornitori;
- ☐ l'invio di messaggi inerenti attività illegali o lo scambio di informazioni riservate su possibili giudizi o cause in corso o la promozione di posizioni o azioni politiche;
- ☐ allegare a messaggi di posta elettronica dati riservati o dati personali senza una adeguata protezione quale la crittografia dell'allegato o l'utilizzo di canali sicuri (SSH o TLS).

11.2 Finalità di utilizzo dei messaggi di posta elettronica

Gli utenti non devono aspettarsi che i materiali composti, inviati o ricevuti tramite i Sistemi di Posta Elettronica Aziendale siano considerati privati o riservati. L'Azienda si riserva la possibilità di

controllare che il contenuto delle e-mail non sia illecito o sia contrario ai propri interessi. Tutti i messaggi creati, inviati, ricevuti e memorizzati da o verso fonti interne o esterne, possono essere oggetto di tali controlli. L'uso di password o cartelle, con nomi personali o comuni, non identificano questi messaggi come "privati" e l'Azienda può riservarsi la possibilità di accedere cartelle qualora lo ritenga necessario, a tutela dei propri diritti ed interessi.



L'uso dei Sistemi di Posta Elettronica per uso personale anche occasionale o fortuito non è consentito, salvo diversa esplicita autorizzazione così come non è consentito utilizzare la posta elettronica per qualsiasi utilizzo non autorizzato dall'azienda.

In alcuni casi i messaggi e-mail possono essere considerati legalmente vincolanti per l'Azienda, in quanto possono essere interpretati come contratti. A tal fine è fatto divieto di fare offerte (servizi, prodotti e impiego) via e-mail senza preventiva autorizzazione.

I messaggi e-mail costituiscono una registrazione permanente di comunicazioni e pertanto gli utenti devono prestare attenzione alla qualità e al contenuto degli stessi. Ciascun utente è Responsabile della lettura e del trattamento delle proprie e-mail con scadenza giornaliera.

Ogni utente avrà cura di cancellare o salvare con regolarità tutti i messaggi non utilizzati.



Si raccomanda vivamente di non aprire messaggi con allegati "sospetti" e ricevuti da sconosciuti, oppure visibilmente frutto di attività "virale"; in tal caso, si richiede di segnalare la presenza di tali messaggi al Servizio ICT per le necessarie verifiche e la messa in atto di eventuali azioni correttive.

11.3 Accesso al sistema di posta elettronica



A nessun utente è permesso controllare o accedere ai messaggi di un altro utente senza la sua preventiva autorizzazione. Eventuali richieste di accesso a messaggi per poter rispondere ad azioni legali o allo scopo di rappresentare l'azienda in eventuali controversie in corso o minacciate, indagini o reclami, devono essere portate all'attenzione della Direzione.

L'uso illecito del Sistema di Posta Elettronica aziendale è proibito e potrà essere oggetto di applicazione delle sanzioni, di cui sopra, applicate dalla società nei confronti dell'utente inadempiente.

Tutte le e-mail interne o provenienti dall'esterno restano di proprietà dell'Azienda che si riserva il diritto di monitorarne l'uso ai fini dell'amministrazione del sistema entro i limiti di legge e di verificarne eventuali contenuti illeciti o contrari alla sua attività.

11.4 Firma dei messaggi di posta elettronica

Le e-mail devono essere firmate, devono cioè comparire in coda al testo del messaggio: il nome, il cognome, il ruolo aziendale e/o l'Area di appartenenza, la ragione sociale dell'azienda di

appartenenza, l'indirizzo della sede legale, il numero di telefono diretto (o quello del centralino di riferimento), il numero di fax, il numero di telefono cellulare aziendale (opzionale).

Gli utenti sono tenuti a configurare tale firma ed a predisporre l'inserimento automatico nelle e-mail.

Gli utenti non devono aggiungere alla propria firma: materiale illustrativo, citazioni, indirizzi web personali o altre informazioni non essenziali, né usare sfondi o aggiungere nuovi stili di carta intestata ai messaggi.

A tutti i messaggi di posta elettronica indirizzati all'esterno dell'Azienda deve essere accodata una *clausola liberatoria* del seguente tenore, conforme alle leggi ed ai regolamenti vigenti:

"Ai sensi del D. Lgs. 196/2003 e del REG. UE 2016/679 le informazioni contenute in questo messaggio di posta elettronica sono di carattere riservato e ad uso esclusivo del destinatario sopra indicato. I dati personali vengono custoditi e controllati in modo da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito. Nell'ambito di tale finalità si informa che è vietato l'uso, la diffusione, distribuzione o riproduzione da parte di ogni altra persona. Nel caso aveste ricevuto questo messaggio di posta elettronica per errore, siete pregati di segnalarlo immediatamente al mittente e distruggere quanto ricevuto (compresi i file allegati) senza farne copia.

Qualsivoglia utilizzo non autorizzato del contenuto di questo messaggio costituisce violazione dell'obbligo di non prendere cognizione della corrispondenza tra altri soggetti, salvo più grave illecito, ed espone il responsabile alle relative conseguenze, ai sensi del del D.lgs 196/2003, REG. UE 2016/679 e del codice penale.

Confidentially notice. This e-mail transmission may contain legally privileged and/or confidential information. Please do not read it if you are not the intended recipient(S). Any use, distribution, reproduction or disclosure by any other person is strictly prohibited. If you have received this e-mail in error, please notify the sender and destroy the original transmission and its attachments without reading or saving it in any manner. Rif. D.l. 196/2003, REG. UE 2016/679 and Penal Code"

Evitare di inoltrare comunicazioni a più riceventi nella stessa e-mail se vengono allegati dati personali

11.5 Protezione contro i virus, malware e spam nell'ambito del sistema di posta elettronica

Il sistema centrale di posta elettronica è fornito di un sistema che controlla i contenuti del messaggio intercettando al meglio delle sue possibilità i messaggi infetti da virus riconosciuti o da malware o da altri elementi sospetti. Ciò nonostante, il criterio non è sicuro in modo assoluto e si possono verificare casi in cui la simulazione del messaggio inganni anche il sistema di protezione. Gli utenti, quindi, devono eliminare tutti i messaggi provenienti da persone non identificate e/o aventi oggetti di dubbio contenuto ed affidabilità. Ove permanga il sospetto di aver ricevuto un

messaggio infettato, gli utenti dovranno contattare immediatamente il Servizio ICT, informando previamente il Responsabile di Funzione.

L'utente potrà consultare, rilasciare, cancellare, aggiungere o togliere l'indirizzo di posta mittente della mail sospetta alla propria white-list, concedendogli di essere sempre riconosciuto come indirizzo valido o alla propria black-list impedendo che venga trattenuto e notificato, ma eliminato direttamente.

Si consiglia periodicamente di svuotare la cartella della Posta indesiderata (spam) per non sovraccaricare la propria cassetta di posta elettronica.

12. NORME DI UTILIZZO INTERNET

L'uso di Internet da parte degli utenti dei sistemi informativi aziendali è regolato da quanto esposto nel presente documento. L'Azienda dispone di strumenti che le permettono di monitorare tale attività, al fine di salvaguardare la sicurezza dei propri dati e dei propri sistemi informativi, in conformità con le leggi vigenti.

Qualsiasi uso improprio o illecito da parte degli utenti e verrà comunicato all'interessato e potrà comportare l'applicazione di sanzioni. Nel caso di utenti dipendenti o assimilati, l'improprio o illecito uso verrà comunicato al proprio Responsabile di Area/Funzione.

Personal computer, notebook, smartphone e tablet assegnati al singolo utente ed abilitati alla navigazione in Internet costituiscono uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

12.1 Accesso ad Internet

L'autorizzazione all'uso di Internet da parte dei singoli utenti viene concessa secondo quanto previsto dalle regole aziendali standard o da specifiche regole definite in funzione della tipologia di servizio.

Si rende noto che la Società può utilizzare appositi strumenti di blocco o filtraggio mediante i quali può bloccare la navigazione su categorie di siti i cui contenuti sono classificati come certamente estranei agli interessi e alle attività aziendali o inseriti in una black list.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:



- ☐ l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione, nel caso di dubbio, dovrà venir a tal fine contattato il Servizio ICT;
- ☐ l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, per motivi non strettamente legati all'attività lavorativa, fatti salvi i casi specificatamente autorizzati dalla Direzione

Generale (o eventualmente dal Responsabile di Area/Funzione) e comunque nel rispetto delle normali procedure di acquisto;

- ☐ ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa con l'indirizzo di posta aziendale usato come identificativo;
- ☐ la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile di Area/Funzione;
- ☐ l'accesso, tramite internet, a caselle webmail di posta elettronica personale;
- ☐ l'attivazione di sistemi di connessione alternativi e non protetti (ad es. modem del telefono in *tethering*) mentre si è collegati in rete aziendale (*wired o wireless*).

È assolutamente vietato accedere a siti Internet che comportino per l'azienda rischi di *responsabilità legale, di sicurezza sui dati e sistemi aziendali, perdita di banda di rete*.

Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT ai sensi di quanto sopra, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy Server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda. Resta inteso che i controlli dovranno essere effettuati esclusivamente al fine di garantire la sicurezza dei dati e la salvaguardia del sistema informatico.

12.2 Download di software



È vietato scaricare programmi applicativi, utilità di sistema operativo, screen saver da Internet. Dove necessario, detti software devono avere la relativa licenza ed essere formalmente registrati presso il Servizio ICT.

È tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore.

13. PROTEZIONE ANTIVIRUS E ANTI-MALWARE

I computer possono essere infettati da virus che causano danni o perdite di dati e programmi, oltre che perdita di tempo e di costi.

I programmi antivirus hanno il compito di riconoscere ed intercettare i virus che infettano i file eventualmente inseriti nel disco fisso del computer da supporti esterni, quali chiavette USB o CD, DVD, in allegato a messaggi di posta elettronica, o scaricati da Internet e di fornire relativa segnalazione all'utente.

Il sistema informatico di Etra S.p.A. è protetto da software antivirus e da firewall centralizzato aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Servizio ICT.

È assolutamente vietato disattivare l'applicativo antivirus e anti-malware. La disattivazione o la rimozione del software di protezione costituiscono una grave violazione alle norme di sicurezza.

14. UTILIZZO DEI TELEFONI, FAX E FOTOCOPATRICI AZIENDALI

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione.

Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. Evitare di inoltrare comunicazioni a più riceventi nella stessa e-mail se vengono allegati dati personali

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di Area/Funzione.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Area/Funzione.

15. NORME SPECIFICHE PER TELELAVORO E SMART WORKING

Nel caso in cui l'utente sia stato autorizzato a svolgere la propria prestazione lavorativa in modalità da remoto, dovranno essere rispettate, oltre alle cautele e le misure di sicurezza previste dalle norme aziendali e già descritte nel presente Regolamento, le seguenti prescrizioni:

- gli utenti dovranno svolgere tutte le operazioni di trattamento dei dati, in forma cartacea o informatizzata, usando la massima riservatezza e nel rispetto delle misure di sicurezza previste dalle *policy* e dalle norme aziendali reperibili nei canali di informazione ufficiali, la cui mancata osservanza può comportare conseguenze giuridiche rilevanti, talvolta anche di natura penale. Il rispetto di talune misure di sicurezza dipende esclusivamente dal

comportamento di ciascun utente, compresa l'osservanza di quanto disposto nel presente Regolamento;

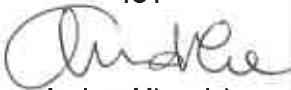
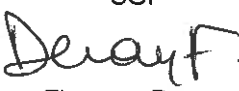
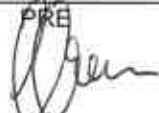
- evitare di inoltrare comunicazioni a più riceventi nella stessa e-mail se vengono allegati dati personali;
- mantenere riservate le chiavi d'accesso, modificandole secondo i termini imposti dall'Azienda, utilizzando password sicure secondo quanto già dettagliato al relativo punto;
- ☐ evitare di accedere a social network o ad altre applicazioni social facilmente *hackerabili* con il dispositivo utilizzato per svolgere la prestazione lavorativa;
- ☐ utilizzare la massima diligenza e operare con la massima riservatezza, soprattutto quando vengono utilizzati sistemi informatici ed elettronici in pubblico o in luoghi aperti al pubblico, onde evitare che i dati o le password possano essere intercettate da soggetti terzi;
- ☐ omettere la trasmissione di informazioni riservate e personali anche a mezzo telefono o canali di comunicazione non aziendali (es. posta elettronica privata);
- ☐ evitare di conservare *files* in locale, salvo nel caso di estrema necessità e urgenza;
- ☐ nel caso in cui si dovesse rendere necessaria la stampa e l'utilizzo di documenti in formato non elettronico contenenti dati funzionali allo svolgimento delle mansioni lavorative, alla conclusione della prestazione lavorativa giornaliera questi dovranno essere eliminati, salvo che non costituiscano originali o comunque documentazione rilevante per la Società e quindi non possano essere distrutti: in tal caso, in via eccezionale, tali documenti dovranno essere conservati in armadi, cassette o altri contenitori muniti di serratura presso il proprio domicilio fino alla loro riconsegna presso la sede della Società;
- ☐ elaboratore fornito in dotazione da parte della Società, anche al fine di evitare l'indebito utilizzo dello stesso da parte di terzi, deve essere spento al termine della sessione di utilizzo e comunque deve essere bloccato in caso di mancato utilizzo o di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo, al fine di evitare che ai dati possano accedere persone non autorizzate presenti nel luogo ove svolge la prestazione fuori sede;
- ☐ l'accesso al dispositivo informatico utilizzato per la prestazione lavorativa sarà consentito, oltre all'utente, al Servizio ICT, al quale questo dovrà rivolgersi per qualsiasi problematica relativa alla strumentazione elettronica ed informatica di cui è dotato;
- ☐ in caso di furto/smarrimento del dispositivo informatico aziendale è necessario informare immediatamente la Società e il Servizio ICT, al fine di attivare le necessarie procedure;
- ☐ utilizzare i dati nei limiti strettamente necessari allo svolgimento dell'attività lavorativa, oltre che vigilare in modo da ridurre al minimo i rischi di distruzione, perdita o indisponibilità, anche accidentale, dei dati, di accesso o modifica non autorizzata o di trattamento non consentito o non conforme alle finalità della raccolta;
- ☐ porre particolare attenzione all'utilizzo di token, smart card e/o badge ed alla loro conservazione affinché non possano essere utilizzati da altre persone;

- ☐ accedere solamente a reti protette da relativa chiave di rete crittografata (wpa, wpe), sia che si tratti di rete Wi-Fi domestica che di hotspot (dati cellulare). In ogni caso è vietato l'accesso alla rete tramite Wi-Fi aperto, hotspot gratuiti o altra forma di connessione alla rete internet non protetta;
- ☐ evitare di trasmettere dati a terzi esterni alla Società, salvo ciò non sia espressamente previsto dalle applicazioni, procedure e processi aziendali. Eventuali eccezioni dovranno ottenere una preventiva autorizzazione scritta del Responsabile di Funzione e/o della Direzione della Società.

16. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dal Responsabile privacy, verificate e approvate dal Direttore Generale e condivise con il Titolare del Trattamento.

Il presente Regolamento è soggetto a verifica, con conseguente ed eventuale revisione nei contenuti, con frequenza annuale.

2	06/6/2023	Integrazioni tecniche e nuove indicazioni Approvato dal Consiglio di Gestione il 06/06/2023	ICT  Andrea Mirandola	DG  Domenico Lenzi
			SGI  Florence Deray	PRE  Flavio Frasson
Rev.	Data	Descrizione modifiche	Redazione	Approvazione