POLITICA

PER

LA SICUREZZA DELLE INFORMAZIONI

Per Verifica e Approvazione Alta Direzione del 01/07/2022

Ing. Parietti

Ing. Romano

E.T.S. S.p.A.
ENGINEERING AND TECHNICAL SERVICES
Sede Operativa: Via Mazzi, 32
24018 VILLA D'ALME' (BG)
Cod. [illegible] - P.IVA 02141540167

1. PREMESSA

Il presente documento descrive le politiche di sicurezza adottate da ETS SpA per garantire:

- la tutela del patrimonio digitale appartenente all'organizzazione rispetto ai rischi di accesso non autorizzato alle risorse informatiche, di perdita o di divulgazione non consentita delle informazioni.
- il rispetto della normativa vigente in materia di riservatezza dei dati personali.

L'adeguamento del comportamento di dipendenti e collaboratori rispetto a quanto indicato contribuirà al raggiungimento degli obiettivi della sicurezza, che si concretizzano nei tre seguenti aspetti principali:

- **Disponibilità**: ovvero garantire sempre l'accesso alle informazioni da parte del personale autorizzato in relazione alle esigenze lavorative;
- **Riservatezza**: ovvero garantire la prevenzione di accessi abusivi o non autorizzati alle informazioni;
- **Integrità**: ovvero, garantire che le informazioni non vengano alterate da incidenti o abusi.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche degli opportuni meccanismi organizzativi; infatti, le misure di natura tecnica, per quanto sofisticate, non risultano efficaci se non utilizzate e controllate in modo adeguato.

2. IL SISTEMA AZIENDALE

Nel rispetto di questi principi, ETS promuove tutte le azioni necessarie affinché i processi e le attività siano orientati al raggiungimento dei seguenti obiettivi:

- Garantire la massima sicurezza delle informazioni dei clienti, in termini di riservatezza, disponibilità e integrità delle informazioni stesse fornendo così un servizio ad alto valore aggiunto, in particolare grazie alla segregazione dei dati di clienti che possono trovarsi in competizione
- Dare continuità operativa ai servizi critici anche a seguito di gravi incidenti
- Tutelare i diritti e gli interessi di tutti coloro che interagiscono con l'azienda (clienti, dipendenti, collaboratori, terze parti, ecc..)
- Salvaguardare gli interessi degli investitori e dei partners
- Garantire un livello di servizio eccellente

3. DESTINATARI

I destinatari della presente policy sono i dipendenti ed i collaboratori di Goddgest che utilizzano la strumentazione informatica messa a disposizione dall'organizzazione per accedere al patrimonio digitale aziendale, elaborarne le informazioni e fornire servizi di supporto ai clienti.

4. SICUREZZA DELLE INFORMAZIONI

4.1 IMPEGNO RISERVATEZZA

Tutti i destinatati si impegnano a rispettare il presente **documento**

Definizioni

Con il termine "*Informazioni Riservate*" (d'ora in avanti anche "Informazioni) si intendono:
tutti gli atti, i documenti, le informazioni, le notizie e i dati, di qualsiasi natura relativi alle aziende clienti di ETS SpA che ci sono state — o che ci saranno — comunicate, e/o comunque rese note, prima o dopo l'assunzione, verbalmente o per iscritto, o che sono state — o che saranno acquisite, in qualsiasi modo, nel corso del lavoro, nonché i documenti, i rapporti, i commenti, le analisi, gli studi, le estrapolazioni, predisposti da noi o dai nostri consulenti che in qualsivoglia maniera contengano o riflettano le suddette informazioni, o siano stati elaborati sulla base delle stesse informazioni.

Obbligo di riservatezza

I dipendenti ETS SpA si impegnano a trattare e mantenere strettamente riservate e segrete le Informazioni ricevute dai clienti, al fine di non pregiudicare in alcun modo la riservatezza delle stesse.

In particolare, ma non in modo esaustivo, i dipendenti assicurano il rispetto degli impegni che la ETS SpA stessa ha assunto con i propri Clienti ovvero:

- considerare strettamente riservate e, pertanto, a non divulgare e/o comunque a non rendere note a soggetti terzi le Informazioni Riservate, intendendosi per "soggetti terzi" tutti i soggetti diversi dai nostri amministratori, dipendenti, intermediari o consulenti;
- ad adottare tutte le cautele e le misure di sicurezza necessarie e opportune, secondo gli standard previsti dalla normativa ISO 27001, al fine di mantenere riservate le Informazioni, nonché al fine di prevenire accessi non autorizzati, sottrazione e manipolazione delle stesse;

- a tenere i contatti unicamente con le persone indicate dal cliente;
- a restituire immediatamente, dietro richiesta da parte del cliente, ogni e qualsiasi documento, analisi, rapporto, valutazione, previsione di cui siamo venuti in possesso nel corso del progetto, senza conservarne alcuna copia;
- ad osservare rigorosamente la normativa vigente in materia di privacy e di protezione dei dati personali.

Utilizzo delle Informazioni

Le Informazioni Riservate dovranno essere utilizzate al solo fine del progetto oggetto del contratto con il cliente

Tutti i destinatari si impegnano quindi ad utilizzare le Informazioni Riservate solamente a tale fine.

Eccezioni

L'Impegno di Riservatezza non si applicherà alle Informazioni Riservate che:

- sono di pubblico dominio per essere state divulgate dalla stampa, dai mezzi di comunicazione di massa in generale, o attraverso ogni altro mezzo elettronico accessibile per la consultazione indistinta al pubblico, purché la divulgazione non derivi da nostro fatto o colpa;
- devono essere obbligatoriamente divulgate per legge, o in virtù di un provvedimento amministrativo.

4.2 POLICY SICUREZZA

Utilizzo del Personal Computer

- Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
- Non è consentita l'attivazione per la prima volta della password d'accesso, senza preventiva autorizzazione da parte Direzione.
- Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte della Direzione

- Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. L'utilizzatore sarà responsabile della buona conservazione, cura e custodia del PC sia in ufficio che durante trasferte esterne.
- Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge (adempimenti amministrativi) o necessarie all'attività lavorativa.
- Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili (.tmp). Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
- E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili.
- Le gestioni locali dei dati dovranno scomparire per essere sostituite da gestioni centralizzate su server.
- Non è consentita l'installazione di programmi diversi da quelli autorizzati dalla Direzione.
- Non è consentita la duplicazione di programmi informatici ai sensi delle normative vigenti
- La Direzione può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli utenti sia sulle unità di rete.

Utilizzo della rete interna

- La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.
- Qualora nella rete interna debbano circolare dati, notizie ed informazioni aziendali, deve essere premura di ciascun dipendente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

Utilizzo della rete internet

- È fatto divieto memorizzare dalla rete documenti, file o dati comunque non attinenti lo svolgimento delle attività aziendali, in particolare:
- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames) potendo esporre a rischi di sicurezza la rete aziendale;

- Si rende noto che la Società ha attivato sistemi di monitoraggio della navigazione aziendale secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, Provvedimento del 1 marzo 2007, effettuando monitoraggio generalizzato dei log di connessione.
- Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della rete societaria verso Internet.
- Eventuali attivazioni di controlli specifici saranno preventivamente notificate.
- I log di connessione di cui sopra, saranno conservati per 15 giorni.

Gestione delle Password

- Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dalla Direzione.
- L'utente è tenuto a conservare nella massima segretezza la password di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione/ autorizzazione.
- L'utente è tenuto a scollegarsi dal sistema o a inserire uno screensaver con password per lo sblocco ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
- La password deve essere immediatamente sostituita, dandone comunicazione alla Direzione nel caso si sospetti che la stessa non garantisca più la segretezza.

Utilizzo di PC portatili

- L'utente è responsabile del PC portatile assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
- Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
- I PC portatili utilizzati all'esterno in caso di allontanamento, devono essere custoditi in un luogo protetto.
- Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.
- Nel caso di accesso alla rete aziendale tramite Accesso Remoto: utilizzare l'accesso in forma esclusivamente personale utilizzare la password non divulgandola a terzi, compresi i membri del nucleo famigliare.

- Disconnettersi dal sistema di Accesso Remoto al termine della sessione di lavoro.
- Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

Uso della posta elettronica

- L'abilitazione alla posta elettronica è incarico al responsabile IT
- La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
- Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
- Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti, questi ultimi non devono essere aperti.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg)
- Nel caso in cui si debba inviare un documento all'esterno dell'Azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf).
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- Le modalità di invio degli allegati sono funzione della loro tipologia e della loro dimensione; pertanto, gli strumenti di trasmissione possono essere: posta elettronica, piattaforme di sharing.
- E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

E.T.S. S.p.A. Engineering and Technical Services
Capitale Sociale 500.000,00 € i.v.
R.E.A. di Bergamo n. 266066
C.F. e P.IVA n. 02141540167
Sistemi Qualità, Sicurezza, Ambiente certificati
UNI EN ISO 9001 | UNI ISO 45001 | UNI EN ISO 14001
Sistema di Gestione BIM conforme UNI PdR 74:2019

Sede Legale:
Via Casalino,18 | 24121 Bergamo

Sede Operativa:
Via A. Mazzi, 32 | 24018 Villa d'Almè (BG)
T +39 035 63 13 111
F +39 035 54 50 66
info@etseng.it | etseng@pec.it | www.etseng.it

Protezione antivirus

- Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..)
- Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale.
- Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer, segnalare l'accaduto al Responsabile dei Sistemi Informativi
- 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 non eliminabile dal software, non dovrà essere utilizzato.

Gestione lavoro da remoto

Per lo svolgimento delle attività da remoto si dovranno rispettare le seguenti indicazioni:

- nel caso di dispositivi di proprietà del dipendente, creare un account separato per le attività lavorative, le cui credenziali siano note unicamente al dipendente medesimo (è esclusa pertanto la condivisione di tali credenziali con i familiari);
- nel caso di dispositivi forniti da ETS SpA, utilizzare solo l'account creato per il dipendente dal gestore della risorsa e solo per scopi di lavoro; è vietata la creazione di ulteriori account, se non su specifica e motivata autorizzazione del responsabile della struttura di appartenenza; è altresì vietata la condivisione delle credenziali, anche con i familiari;
- i dati trattati durante l'attività lavorativa devono essere accessibili unicamente al dipendente;
- configurare la modalità di blocco automatico dell'accesso al sistema dopo un breve periodo di inattività o bloccare manualmente l'accesso al sistema quando il dispositivo non è in uso;
- effettuare sempre il logout dai servizi Web una volta terminata la sessione lavorativa;
- custodire adeguatamente le credenziali di accesso e non condividerle con terzi;
- custodire con le debite cautele i dispositivi in uso;
- effettuare sempre il logout da programmi, VPN e piattaforme di lavoro al termine della sessione lavorativa;
- non aprire allegati ricevuti via mail da mittenti sconosciuti oppure file scaricati da Internet che potrebbero contenere codice malevolo;

- non introdurre consapevolmente software malevolo sulla rete o sui dispositivi utilizzati per lo smart working;
- non collegare i dispositivi in uso a reti e VPN sconosciute;

Gestione postazione di lavoro (politica Scrivania pulita)

1. Migliorare l'aspetto degli uffici: quando le scrivanie sono pulite ed esenti da carta e disordine, l'ufficio si presenta più pulito ed efficiente. Le persone si sentono più a loro agio in un ambiente ben organizzato e gli ospiti avranno una buona sensazione della società.

2. Migliorare la protezione dei dati sensibili: molte informazioni nella nostra azienda sono confidenziale e devono essere protette da accessi non autorizzati da parte di soggetti interni o esterni.

3. Migliorare la produttività: la Direzione è fermamente convinta che una "politica Scrivania pulita" aumenterà la produttività, perché ci vorrà meno tempo dedicato alla ricerca di oggetti. Aiuta a focalizzare e mantenere una mente chiara.

4. Postazioni utilizzabili: con l'attuazione della "politica Scrivania pulita" è possibile condividere scrivanie tra diversi impiegati. Questo riduce i costi di infrastruttura e aumenta la flessibilità di cambiare posto a seconda dei progetti o programmi.

Al fine di attuare la "politica Scrivania pulita" vi invitiamo a seguire tre regole fondamentali:

1. Quando si è alla propria scrivania: tieni sulla scrivania ciò di cui hai bisogno nella giornata (documentazione relativa al lavoro che stai svolgendo).
2. Quando si lascia temporaneamente la scrivania: quando lasci la tua scrivania per riunioni o pause, controlla se ci sono informazioni sensibili sulla tua scrivania e mettile via. Inoltre, poni in stand-by o inserisci lo screen saver sul tuo Pc proteggendolo con password per lo sblocco.
3. Quando si esce da lavoro: la sera non lasciare documenti sulla scrivania, la documentazione deve essere riposta nei cassetti o negli armadi a disposizione (chiusi con chiave).

Gestione segnalazioni incidenti riguardanti la sicurezza delle informazioni

Al fine di attuare la "sicurezza delle informazioni" ovvero conservare la riservatezza, l'integrità e la disponibilità delle informazioni, ti invitiamo a segnalare al Responsabile dei Sistemi Informativi ogni evento o incidente relativo alla sicurezza delle informazioni secondo le modalità descritte nella POL A16, per la gestione delle azioni necessarie.

Si riportano nel seguito le definizioni di evento ed incidente relativo alla sicurezza delle informazioni:

B. Evento relativo alla sicurezza delle informazioni: un identificato accadimento relativo allo stato di un sistema, servizio o rete, indicante una possibile violazione della politica per la sicurezza delle informazioni, un malfunzionamento delle contromisure o una situazione mai osservata in precedenza, che possa interessare la sicurezza.

C. Incidente relativo alla sicurezza delle informazioni: evento o serie di eventi relativi alla sicurezza delle informazioni, non voluti o inattesi, che hanno una probabilità significativa di compromettere le operazioni relative al business e di minacciare la sicurezza delle informazioni.

Esempi di eventi ed incidenti sono i seguenti:

- Malfunzionamento HW
- Segnalazione Virus
- ecc.