PS 02 Politica della sicurezza delle informazioni

0	RSGI		DIR		01.03.2025
Rev.	**Funzione**		**Funzione**		**Data**
	Redazione/verifica		**Approvazione/emissione**		

1 SCOPO

Scopo della presente Procedura è definire e descrivere i criteri, le responsabilità e le modalità operative necessare alla conformità alla nuova norma ISO 27001:2022. Il documento integra i requisiti definiti negli altri documenti aziendali.

La presente procedura si applica a tutte le tipologie di attività svolte dall'organizzazione.

2 ACRONIMI E DEFINIZIONI

Acronimo	Definizione
SGI	Sistema di Gestione Integrato
RSGI	Responsabile SGI

3. DOCUMENTI DI RIFERIMENTO

Norma UNI EN ISO 9001:2015
Norma UNI CEI ISO/IEC 27001:2022

4. RESPONSABILITÀ E ISTRUZIONI PER LA SICUREZZA DELLE INFORMAZIONI

JUSTBIT si è dotata di un Sistema di Gestione per la Sicurezza delle Informazioni secondo quanto previsto dalla norma ISO/IEC 27001. Pertanto il personale dipendente e/o collaboratori e tutti coloro che, a vario titolo, lavorano e/o con l'azienda si impegnano ad adottare misure adeguate contro l'accesso non autorizzato, la divulgazione, il trattamento, la perdita o distruzione delle Informazioni, inclusa ogni attività di prevenzione o almeno di minimizzazione dei rischi di qualsiasi furto, manipolazione, appropriazione indebita, uso improprio delle Informazioni; ciò include, senza limitazioni: (i) l'adozione di procedure, nonchè di misure tecniche ed organizzative; (ii) l'utilizzo di sistemi IT e controlli di sicurezza all'avanguardia; (iii) il rispetto delle misure di sicurezza sulla base del livello di classificazione attribuito e individuato secondo ALLEGATO "B" - Classificazione e etichettatura delle informazioni" di cui alla allegata Appendice o, se diverso, come attribuito e comunicato dal Committente; (iv) l'adozione di misure, ivi incluse regole e meccanismi di gestione dell'identità/identificazione e dell'accesso/autenticazione nonchè regole idonee a salvaguardare la disponibilità, l'integrità e la riservatezza delle Informazioni.

In aggiunta a quanto sopra, ove applicabile, le parti interessate dovranno mantenere misure di sicurezza tecniche ed organizzative e rispettare le disposizioni e le tempistiche relative agli Incidenti di sicurezza fatte salve le ulteriori disposizioni in materia di violazione della sicurezza dei dati personali di cui all'eventuale Accordo sul Trattamento dei Dati (ove esistente).

Questa policy definisce gli standard e le regole di utilizzo da parte dei dipendenti e dei collaboratori di JUSTBIT della posta elettronica, di Internet, delle dotazioni IT, dei programmi e dei sistemi informatici aziendali. Tali standard sono concepiti al fine di garantire che le reti, le strutture IT e il patrimonio digitale di JUSTBIT siano utilizzati con modalità sicure e responsabili, al fine di garantire la riservatezza, l'integrità e la disponibilità dei sistemi e delle informazioni di JUSTBIT, nonché al fine di assicurare un trattamento legittimo dei dati personali del personale di JUSTBIT.

Non rientra tra gli scopi di questa policy il controllo a distanza e/o in forma occulta delle opinioni, abitudini e/o dell'attività dei lavoratori, che rimangono strettamente vietati e non consentiti.

La presente policy informa altresì sulle modalità con le quali JUSTBIT, in qualità di datore di lavoro, può legittimamente controllare e segnalare l'uso abusivo del sistema informatico aziendale, nonché effettuare indagini in relazione a sospette violazioni dei sistemi da parte del personale o di terzi, o a condotte illegittime.

Questa policy e le relative istruzioni integrano dunque: (i) l'informativa sul trattamento dei dati personali di dipendenti e collaboratori ai sensi dell'art. 13 del GDPR; e (ii) le istruzioni già fornite al personale e ai collaboratori nella lettera di designazione ai "soggetti autorizzati al trattamento". Questa policy costituisce anche espressione dei doveri di correttezza comportamentale e diligenza contrattuale e costituisce parte integrante del complessivo sistema normativo aziendale.

La presente policy si applica a tutti i dipendenti, il personale, i collaboratori, i consulenti di JUSTBIT, i quali utilizzano un account aziendale, un sistema di posta elettronica aziendale, o qualsiasi dispositivo connesso alla rete di JUSTBIT. La presente policy si applica inoltre a ciascun utente dei sistemi di navigazione, messaggistica istantanea, VoIP, sistemi cloud, sistemi di trasferimento o condivisione di file di JUSTBIT, nonché altri protocolli standard di proprietà del consorzio, backup, o banche di dati.

JUSTBIT esige che tutte le proprie risorse siano utilizzate in modo professionale. JUSTBIT fornisce a proprie spese tali risorse per i suoi scopi aziendali. È dovere di ciascun Utente assicurare che tale tecnologia sia utilizzata per scopi aziendali adeguati e con modalità tali da non danneggiare in alcun modo JUSTBIT o il suo Personale.

Tutti gli Utenti di JUSTBIT sono tenuti ad assicurare che i dati siano acquisiti, archiviati e trattati adeguatamente e che l'utilizzo delle dotazioni elettroniche aziendali sia conforme alla presente policy. Ciascun team che abbia a che fare con dati personali deve garantire che gli stessi siano trattati in linea con la presente policy e con i principi in materia di protezione dei dati, anche conformemente alle ulteriori istruzioni fornite agli specifici soggetti autorizzati al trattamento dei dati personali.

Accesso ai dati da parte di soggetti non autorizzati al trattamento – Occorre sempre controllare ed evitare che l'accesso ai dati trattati da JUSTBIT in qualsiasi contesto possa avvenire da parte di persone non autorizzate al trattamento (interni o esterni alla organizzazione aziendale). Il dato deve, innanzitutto, essere protetto da accessi non autorizzati, che possono avvenire di persona (si pensi a un soggetto non autorizzato che entra fisicamente in un ufficio e prova a conoscere o sottrarre dati) o tramite contatti telematici che possono rivelarsi truffaldini (ad esempio un'email o altra forma di presa di contatto mediante la quale si provino a raccogliere determinati dati o informazioni – si veda l'Allegato A a questo proposito).

Politica di clear screen e clear desk - Si raccomanda di non lasciare incustoditi e accessibili i dispositivi elettronici durante una sessione di trattamento di dati personali, in particolare qualora sia necessario allontanarsi temporaneamente dal posto di lavoro. In caso di assenza momentanea dal proprio posto di lavoro, ci si deve accertare che la sessione di lavoro non sia accessibile a terzi, facendo logout o attivando il salvaschermo (screensaver) con blocco della sessione protetta da credenziali di autenticazione. Si ricorda che la pressione contemporanea dei tasti Ctrl + Alt + Canc attiva la finestra di "Protezione di Windows" dalla quale è possibile premere il pulsante "Blocca computer" per bloccare la postazione di lavoro senza la necessità di uscire dai programmi in uso.

Per cautelarsi ulteriormente dalle eventualità di lasciare sessioni incustodite, il sistema blocca automaticamente, dopo pochi minuti di inutilizzo, le postazioni di lavoro, chiedendo l'inserimento della password in fase di ripristino. La postazione di lavoro deve essere configurata in modo che sia impostato l'avvio automatico dello screensaver ("salvaschermo") dopo al massimo 5 minuti di inattività del personal computer.

Antivirus e firewall - Tutti i computer, sia desktop sia portatili, devono avere installato e attivo il software antivirus, con firewall attivato e devono essere mantenuti costantemente aggiornati con le patch di sicurezza del sistema operativo e degli applicativi utilizzati. Tali aggiornamenti sono, nella maggior parte dei casi, automatici e non richiedono l'intervento dell'Utente. Non bisogna però, salvo casi eccezionali, bloccare o ritardare un aggiornamento dei software o dei sistemi, ma è necessario procedere immediatamente al salvataggio dei file eventualmente aperti e acconsentire all'aggiornamento.

Cifratura dei dati - La cifratura dei file system e degli smartphone, nonché dei supporti esterni, aiuta a difendersi da eventuali data breach, così come l'uso di credenziali forti (lunghezza idonea, formata da lettere

maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'Utente). È quindi obbligo per ciascun dipendente seguire le istruzioni che verranno di volta in volta impartite da JUSTBIT in merito all'adozione della cifratura dei dati che gestisce e adottare credenziali robuste per l'accesso a tali sistemi.

Trasferimento dei dati solo tramite modalità e protocolli sicuri – In caso occorra trasferire dati all'esterno, particolarmente se di natura delicata, occorre utilizzare soluzioni di trasmissione sicura, quali il "Trasferimento di File" in modalità FTP "sicuro" o equivalente dal punto di vista della sicurezza del trasporto, garantendo la cifratura del canale di trasmissione dei dati (ad esempio, utilizzando meccanismi quali le reti private virtuali o la cifratura delle sessioni di trasferimento dei dati). Nel caso di invio di dati di natura particolarmente delicata via e-mail (come definite nell'allegato "B"), la spedizione del file deve avvenire come allegato o link, il quale dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione da parte di soggetti diversi dal destinatario che potrà consistere, a seconda della delicatezza dei dati, in una password per l'apertura del file o in una chiave crittografica rese note agli interessati attraverso separata comunicazione. Nell'invio delle e-mail gli utenti devono essere molto attenti nel controllare l'indirizzo del/i destinatario/i prima dell'invio per evitare errori di battitura o errori dovuti all'autocompilazione. L'invio di comunicazioni deve avvenire solo da device protetti da antivirus onde proteggere le comunicazioni da eventuali malware.In caso di trasferte fuori dall'ufficio, utilizzando i device in ambito pubblico, è necessario prestare la massima attenzione che non vi siano terzi non autorizzati che possano accedere ai dati.

Gestione dei supporti removibili - Qualsiasi supporto di memorizzazione rimovibile eventualmente utilizzato (l'utilizzo dovrà essere autorizzato preventivamente dalla Direzione) dovrà essere dotato di sistemi di accesso di sicurezza atti ad assicurare, in caso di eventuale furto o smarrimento, l'impossibilità per soggetti estranei di poter accedere ai dati negli stessi contenuti. Tali supporti, quali CD/DVD/chiavi/dischi USB, sono da utilizzare solo in caso di mancanza di alternative, ed è necessario riporli in luoghi adeguatamente protetti non appena terminato il loro utilizzo e in caso debbano riutilizzati per altri scopi devono essere preventivamente formattati. Qualora siano da rottamare, vanno prima fisicamente distrutti.

Data breach - L'art. 33 del GDPR impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (data breach) entro 72 ore dal momento in cui ne viene a conoscenza. Per maggiori informazioni occorre consultare l'apposita Data Breach Procedure aziendale. L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche. Qualora, poi, il rischio fosse elevato oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato. Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio. L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto comporta il rischio di sanzioni. Per "data breach" o "violazione di dati" si intende"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Esempi di data breach sono:

i. Furto di credenziali di autenticazione a seguito di un attacco di phishing

ii. Smarrimento di una chiavetta USB o sottrazione di un pc con conseguente perdita di documenti contenenti dati personali

iii. Eliminazione accidentale o pubblicazione indesiderata su internet di un database

iv. Accesso ad informazioni riservate da parte di utenti non autorizzati

Cosa fare in caso di data breach? Tutti gli Utenti devono collaborare alla identificazione e segnalazione di possibili data breach. Nel caso in cui l'Utente sia venuto a conoscenza o sospetti sia avvenuta una violazione dei dati è tenuto ad avvisare tempestivamente il suo superiore o il Team Privacy.

5. CONTROLLI, PRINCIPI DI CORRETTEZZA E PROPORZIONALITÀ

Periodicamente, JUSTBIT può condurre indagini interne (i) casuali e saltuarie, al fine di verificare il rispetto della presente policy o in caso di malfunzionamenti e anomalie; o (ii) mirate, nel caso di sospetto di attività abusive o illegittime o di violazioni dei doveri connessi al rapporto di lavoro. I dati e le informazioni contenuti nelle dotazioni IT possono essere utilizzati da JUSTBIT per tutti i fini connessi al rapporto di lavoro quali scopi disciplinari, per controllare la regolare esecuzione del rapporto di lavoro, il rispetto della presente policy, tutelare il patrimonio aziendale e per salvaguardare le esigenze operative di JUSTBIT.

I controlli saranno eseguiti secondo i principi di proporzionalità, pertinenza, riduzione al minimo dei dati, e necessità, nel rispetto della dignità e dei diritti fondamentali dei lavoratori, nonché in conformità alla presente policy e alle leggi applicabili in materia di protezione dei dati personali.

I file di log di alcuni programmi aziendali sono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e di norma per un periodo massimo non superiore a 3 mesi.

Nei casi in cui si debba far fronte a particolari esigenze tecniche o di sicurezza oppure si debbano utilizzare i dati registrati con riferimento all'esercizio o alla difesa di un diritto in sede giudiziaria (azioni da parte di terzi o viceversa,o in caso di verifiche relative ad un presunto comportamento illecito), oppure si ottemperi all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta di un'autorità, tale periodo verrà prolungato secondo le necessità del caso e nel pieno rispetto delle finalità descritte. Ove possibile, i dati relativi ai file di log sono acquisiti in modalità anonima e quindi non riconducibili direttamente all'identità dei singoli utenti che li hanno generati.

6. FILTRAGGIO WEB - MISURE PREVENTIVE PER RIDURRE NAVIGAZIONI ILLECITE

JUSTBIT potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list implementati ad esempio attraverso i sistemi di content filter dei firewall.

7. USO DI PROGRAMMI DI UTILITA' PRIVILEGIATI

L'uso di programma di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema sono, in generale, vietati.

Tali programmi possono essere utilizzati solo se sussistono le seguenti condizioni:

1. I programmi in questione sono stati autorizzati esplicitamente dalla Direzione;

2. Gli incaricati ad utilizzare tali programmi sono stati oggetto di esplicita autorizzazione da parte della Direzione;

3. Ogni volta che i programmi devono essere utilizzati è necessario che l'incaricato autorizzato richieda alla direzione l'autorizzazione allo specifico utilizzo;

4. Ogni utilizzo di tali programmi deve essere tracciato;

5. I programmi di utilità devono essere disinstallati una volta terminato l'utilizzo

8. CHANGE MANAGEMENT

Il processo di Change Management si compone di 7 fasi:

1. Richiesta della modifica;
2. Valutazione dell'impatto;
3. Procedura Back-out;
4. Approvazione;

5. Implementazione;
6. Test;
7. Chiusura della richiesta.

RICHIESTA DELLA MODIFICA: Le richieste di modifica possono essere effettuate da chi individua l'esigenza di modifica e miglioramento del processo, in coordinamento con il responsabile del dipartimento di riferimento. Tutte le richieste di modifica devono essere registrate e monitorate nel sistema di Change Management, Service Desk. La richiesta deve essere presentata in modo tempestivo includendo tutte le informazioni necessarie.

VALUTAZIONE DELL'IMPATTO: La valutazione dell'impatto deve essere condotta per individuare l'impatto potenziale ed il rischio associato alla modifica richiesta. Il risultato della valutazione serve per avere una maggiore comprensione delle precauzioni necessarie da implementare nel corso dell'attuazione della richiesta. La valutazione dell'impatto deve contenere una breve descrizione delle possibili conseguenze della modifica richiesta ed indicare il numero di risorse che possono essere impattate e/o coinvolte.

PROCEDURA DI ROLL-BACK: Per ogni modifica deve essere prevista e sviluppata una procedura di Roll-back per garantire un ritorno allo status precedente nel più breve tempo possibile.

APPROVAZIONE: L'approvazione è volta a verificare che tutte le fasi definite nel processo di richiesta siano state effettuate e siano adeguate in considerazione del rischio, della sicurezza e dell'impatto che la modifica può avere sull'organizzazione. Tutte le modifiche devono essere approvate secondo lo schema seguente, si riporta a titolo di esempio il solo dip.to Operations. Nell'eventualità di proteggere infrastrutture o sistemi critici per il business, personale autorizzato può implementare cambiamenti d'emergenza e richiedere l'approvazione formale a posteriori. Ogni modifica che può comportare la possibilità di bypassare le restrizioni di sicurezza, deve essere approvata.

IMPLEMENTAZIONE: La fase di implementazione stabilisce un meccanismo attraverso il quale le modifiche possono essere applicate in modo efficace e secondo alti standard di qualità e consente di rimuovere interamente la modifica apportata (procedura di back out), se necessario, senza influire negativamente sulla capacità del sistema di operare come prima della modifica.

TEST: Immediatamente dopo l'implementazione, la modifica deve essere testata per assicurarne la funzionalità operativa. In caso di esito negativo del test deve essere eseguita la procedura di back out oppure rivista l'implementazione.

CHIUSURA DELLA RICHIESTA: Solo a seguito di esito positivo del test di funzionalità operativa e dell'aggiornamento dei documenti relativi alla configurazione (ove necessario), la modifica ed il relativo ticket può essere chiuso.

9. PREVENZIONE DELLA FUGA DI DATI

La perdita di dati può essere definita come l'accesso non autorizzato, la trasmissione o l'estrazione di informazioni da parte di personale e sistemi interni ed esterni o entità malintenzionate che prendono di mira i sistemi informativi di un'organizzazione. La perdita di dati è un rischio che dobbiamo affrontare in tutti i modi possibili e un fattore importante per proteggerlo è essere in grado di rilevare quando vengono sottratti dati riconoscibili. Questa politica si applica a tutti i canali di potenziale fuga di dati, compresi quelli verbali, i social media e quelli che coinvolgono formati fisici come la carta.

La prevenzione dei dati è supportata da controlli di sicurezza standard, ad esempio, misure per limitare l'accesso degli utenti a determinate informazioni (controllo degli accessi logici e fisici) e per la gestione sicura dei documenti cartacei. Tali controlli devono essere integrati da regolari attività di sensibilizzazione degli utenti che informino gli utenti sulla natura della perdita di dati e su come evitarla. Azioni fisiche non autorizzate come fotografare o acquisire screenshot di dati sensibili non sono consentite e tutti i dipendenti di JUSTBIT hanno la responsabilità di segnalare tali casi alla Direzione.

10. VIOLAZIONI, SANZIONI E PROCEDIMENTO DISCIPLINARE

1. Gli utenti sono tenuti a rispettare la presente policy e sono responsabili del corretto e legittimo utilizzo delle dotazioni IT e del trattamento dei dati e delle informazioni aziendali.

2. Le violazioni della presente policy possono essere sanzionate in base all'esito della procedura disciplinare. A titolo esemplificativo, a seconda della gravità dell'esito, la procedura disciplinare potrebbe comportare il licenziamento del dipendente interessato.

3. L'eventuale tolleranza da parte della Società nei confronti di condotte in contrasto con la presente policy, non potrà essere considerata come una tacita abrogazione della stessa, né come una rinuncia di JUSTBIT ad esercitare i propri diritti. Resta ferma la responsabilità di ogni Utente sia civile - per eventuali danni causati a JUSTBIT, ai suoi dipendenti, collaboratori o a terzi - sia penale.

5. Ai fini disciplinari, la presente policy sarà esposta in luogo accessibile a tutti.

11. MASCHERAMENTO E ANONIMIZZAZIONE DEI DATI

Tutti i dati utulizzati per lo sviluppo e la gestione del ciclo di vita del sw sono mascherati e prevedono l'anonimizzazione. Non si usano dati reali dei clienti se non per la fase di validazione e previa approvazione per la gestione e come previsto dai contratti e requisiti.

12 SVILUPPO SICURO

Per lo sviluppo sicuro si adottano standard internazionali ad es. OWASP e il documento di riferimento "Linee guida per lo sviluppo sicuro di codice"

ALLEGATO A

ISTRUZIONI PER PROTEGGERSI DA PHISHING E DA RANSOMWARE

1. JUSTBIT dispone che ogni Utente che abbia accesso a dati, li consulti, li archivi, li diffonda, li modifichi, li raccolga o, comunque, effettui qualsiasi operazione su informazioni, sia in formato elettronico che cartaceo, riferite a persone, al fine di evitare frodi, attacchi informatici e furto di credenziali, si attenga, nell'attività quotidiana, alle seguenti istruzioni.

2. Tali istruzioni sono da considerarsi, a tutti gli effetti, quali direttive aziendali e, in quanto tali, il loro mancato rispetto potrebbe generare delle responsabilità a carico del'Utente.

Il **phishing** è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente. La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc. In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare.

Il **ransomware** è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, "ransom") da pagare per "liberarli". Anche se in alcuni casi

(non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che: (i) sembrano apparentemente provenire da soggetti conosciuti e affidabili (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da persone fidate (colleghi di lavoro, conoscenti); (ii) contengono allegati da aprire (spesso "con urgenza"), oppure link e banner da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli.

È possibile che il servizio di posta elettronica aziendale, pur essendo protetto da strumenti che applicano politiche antivirus e antispam, possa non bloccare una serie di email potenzialmente malevole. Occorre Pertanto osservare le seguenti istruzioni:

Non utilizzare l'email aziendale per scopi personali

Non rispondere mai a e-mail che richiedano dati

Mantenere un atteggiamento sospettoso e prudente nella lettura delle mail e soprattutto nell'apertura degli allegati

Verificare sempre ortografia e sintassi nel testo delle e-mail ricevute

Diffidare di mail che mettono urgenza, che minacciano sanzioni, che promettono premi e vincite o che contengono richieste di aiuto

Non cliccare su link contenuti nel corpo delle e-mail

Non vergognarsi per la truffa subita e segnalare subito l'incidente

Adoperare particolari cautele anche nel caso di mail provenienti (apparentemente) da mittenti noti

Diffidare anche di e-mail personalizzate

Cosa fare nei casi dubbi

In caso di e-mail che desta sospetto, il miglior modo di agire è quello di non fare nulla, non rispondere, non aprire allegati, non cliccare su link, non inoltrare la e-mail a colleghi. Informare invece il proprio responsabile del messaggio sospetto.

Per maggiori informazioni v. anche la pagina tematica pubblicata dal Garante Privacy al seguente indirizzo:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5779928

https://www.garanteprivacy.it/temi/cybersecurity/ransomware

ALLEGATO B

CLASSIFICAZIONE E ETICHETTATURA DELLE INFORMAZIONI

La politica di JUSTBIT sulla protezione dei beni aziendali prevede che gli amministratori, dirigenti e dipendenti, nonchè consulenti e business partner proteggano ed utilizzino i beni di JUSTBIT efficientemente ed in maniera consona agli interessi della stessa.

I beni aziendali includono ovviamente anche le informazioni aziendali, in qualunque forma (cartacea, elettronica, versione originale, copie).

Qualsiasi informazione, conoscenza e dato acquisito o trattato presso JUSTBIT, appartiene alla società stessa e deve essere gestito in maniera conforme alle presenti linee guida. Ogni collaboratore/dipendente, consulente e business partner è responsabile di classificare e proteggere la documentazione che produce/gestisce e di rispettare la protezione richiesta dalla classificazione della documentazione che riceve. La classificazione della documentazione è determinata in base alla valutazione di possibili perdite finanziarie, di competitività o di immagine o in base agli impatti legali a cui JUSTBIT andrebbe incontro in caso di divulgazione non autorizzata dell'informazione.

Una volta classificate, le informazioni devono essere protette con appropriati punti di controllo; quanto più sensibile è l'informazione, tanti più punti di controllo sono richiesti. La classificazione o etichettatura deve essere posta in apice/pedice di ogni pagina del documento. Quando si condividono via email documenti riservati o privati, è buona norma non inviarli in allegato, ma tramite piattaforme condivise quali ad esempio OneDrive, inserendo solamente il link nel corpo dell'email.