ARKIVIA PROJECT Srl

POLITICHE SPECIFICHE DELLA SICUREZZA DELLE INFORMAZIONI (PSSI)

Ed 2 Rev. 2	Del 10-01-2023

Premessa

Il presente documento che integra la Policy aziendale sulla Sicurezza delle informazioni, ha lo scopo di regolamentare, laddove non espressamente previsto nel Manuale del Sistema di Gestione per la Sicurezza delle Informazioni, nelle Procedure o nelle Istruzioni Operative, le prassi comportamentali dei dipendenti dell'organizzazione in merito ad aspetti specifici della sicurezza delle informazioni.

I contenuti sono da intendersi come Linee Guida comportamentali cui i dipendenti tutti devono attenersi scrupolosamente al fine di garantire la sicurezza delle informazioni trattate dall'organizzazione per conto dei clienti, dei fornitori, di parti eventualmente interessate e della stessa organizzazione.

Politica per l'utilizzo dei PC, delle attrezzature e delle infrastrutture aziendali

In considerazione del fatto che per la fornitura dei servizi ai propri clienti, ARKIVIA PROJECT utilizza PC, attrezzature e infrastrutture che costituiscono una cospicua parte del patrimonio aziendale cui l'azienda attribuisce un valore più o meno elevato, la direzione aziendale ha stabilito alcune regole fondamentali per la salvaguardia degli stessi.

Utilizzo dei PC

- A seconda delle esigenze lavorative il dipendente ARKIVIA PROJECT è assegnatario di un Personal Computer Desktop ed è responsabile del corretto utilizzo dello stesso.
- Il software installato su ciascun PC deve essere regolarmente autorizzato dall'azienda e dotato di licenza d'uso.
- La configurazione del PC viene effettuata al momento dell'acquisto e può successivamente essere modificata solo da SGSI.
- Ogni guasto/malfunzionamento deve essere prontamente registrato e gestito secondo le modalità descritte nell'apposita procedura.
- *Non è consentito, agli assegnatari dei PC, senza formale autorizzazione (sono esclusi dal provvedimento autorizzativo RSGI e RD), collegare agli stessi, dispositivi di memoria esterni* (CD ROM, CD RW, USB Pen, HDD esterni).
- La riconsegna del PC per alienazione, riutilizzazione o per manutenzione deve essere preceduta dalla cancellazione dei dati.

Utilizzo delle attrezzature di processo (Server, Fotocopiatrici, stampanti, fax, ecc.)

- Le attrezzature di processo sono a disposizione di tutto il personale dipendente. Il corretto utilizzo è demandato alla sensibilità dei singoli utilizzatori.
- Chiunque riscontri un guasto/malfunzionamento alle apparecchiature è tenuto a segnalarlo tempestivamente in amministrazione che di concerto con RSGSI provvederà al ripristino della funzionalità attraverso l'intervento di *personale interno o esterno abilitato*.

Infrastrutture aziendali

- Al dipendente ARKIVIA PROJECT è consentito l'utilizzo di una postazione di lavoro che in generale è costituita da: tavolo, sedia, armadio e/o cassettiera. Alla postazione di lavoro in generale sono aggiunte, se necessarie per il lavoro richiesto, le infrastrutture e le utilities aziendali (Rete LAN, rete fonia fissa, gruppo di continuità, nonché l'impianto di climatizzazione e l'impianto di rilevazione fumo). A ciascun dipendente è demandato il loro corretto utilizzo.

Ogni utilizzo difforme dai contenuti della presente politica sarà perseguito dalla direzione con provvedimenti disciplinari.

Politica per l'utilizzo dei computers portatili (Personal Portatili, Palmari ecc) e dispositivi rimovibili

L'utilizzo dei computer portatili deve essere espressamente autorizzato dall'organizzazione.
La connessione alla rete aziendale all'interno dell'organizzazione è consentita nel rispetto delle regole stabilite dall'amministratore della rete.
Valgono per i computers portatili, oltre alle regole generali previste per tutte le altre tipologie di computers, le seguenti regole:

- Non lasciare mai incustodito il dispositivo.
- Utilizzare, laddove possibile, lucchetti e cavi di sicurezza (Es. Kensington lock) per impedirne il furto.
- L'eventuale etichettatura del dispositivo stesso con il nome dell'azienda o dell'utente, sarà a cura dell'Azienda.
- In caso di trasporto del PC portatile in auto (che deve essere dotata di capote rigida), in occasione della sosta (che deve essere effettuata in una rimessa chiusa a chiave o in un parcheggio custodito), l'auto deve essere chiusa a chiave, il PC deve essere riposto in bagagliaio chiuso a chiave secondo quanto riportato nell'assicurazione contro il furto stipulata ("Tutti i rischi dell'informatica").
- *In caso di trasporto delle unità rimovibili di Back-up (su unità esterne HDD, su CD-ROM o DVD) o di dati trasportati su supporti removibili (USB Pen, CD-ROM, DVD) prima del trasporto si avrà cura di inserire una pwd o a crittografare i dati e le informazioni contenute al fine di prevenire la perdita di riservatezza, disponibilità derivabili dal furto/smarrimento del dispositivo e si applicano le stesse regole del trasporto in auto dei PC portatili di cui al punto precedente.*
- Sfilare eventuali dispositivi di memorizzazione portatili USB quando si lascia il computer abbandonato per un certo tempo.
- Non aprire i contenuti di dispositivi di memoria (USB Pen, CD-ROM ecc) senza aver effettuato una scansione con il programma antivirus.
- Configurare correttamente i dispositivi Wireless e Bluetooth, specificandone le regole di accesso.

Al fine di prevenire una divulgazione non autorizzata, nonché la modifica dei contenuti, o addirittura la distruzione o la sottrazione delle informazioni contenute in supporti removibili (Dischi esterni, USB Pen, Floppy Disk, CD-ROM ecc) il personale aziendale deve attenersi nel loro utilizzo alle seguenti istruzioni:

- Limitarne l'uso, ove possibile, e procedere alla cancellazione delle informazioni dopo l'utilizzo e se non più necessarie.
- Non lasciare mai incustodito il dispositivo.
- Riporre il dispositivo negli appositi armadi o cassettiere muniti di serratura.
- In caso di dismissione provvedere alla formattazione e alla distruzione fisica dello stesso.

Politica per l'utilizzo del software e per il rispetto del copyright

In considerazione delle politiche per la protezione diritti di proprietà intellettuale imposte dalla comunità internazionale attraverso la legislazione nazionale ed internazionale, l'organizzazione ha stabilito alcune regole fondamentali per assicurare la conformità a requisiti legislativi, cogenti e contrattuali sull'uso del materiale sul quale potrebbero gravare diritti di proprietà intellettuale e l'uso di prodotti software di proprietà.
Per il rispetto delle stesse regole la direzione aziendale ha stabilito di effettuare periodici controlli per verificare il corretto uso del software.

- Su tutti i PC aziendali è tassativamente proibito l'utilizzo di software pirata e/o privo di licenza d'uso.
- È consentito installare sui sistemi di elaborazione soltanto software preventivamente autorizzato dall'Amministratore di Sistema sia esso di tipo commerciale che open source.
- Le licenze d'uso relative al software installato sui PC aziendali, ivi comprese quelle relative al software open source, sono custodite da RSGSI.
- L'installazione di software scaricato gratuitamente da Internet, previa autorizzazione dall'Amministratore di Sistema, è consentita purché l'installazione dello stesso non influisca negativamente sulle prestazioni della macchina e non sia di dimensioni tali da occupare consistenti blocchi di memoria.
- L'assegnatario del software è responsabile dell'installazione degli aggiornamenti, laddove presenti, sul proprio elaboratore.
- È tassativamente proibita la duplicazione del software su licenza con qualsiasi mezzo (CD-ROM, USB Pen, HDD Esterni) o il trasferimento dello stesso su altri PC attraverso la rete aziendale o altri dispositivi di comunicazione.
- È proibito duplicare, convertire in un altro formato o estrarre registrazioni commerciali (filmati, audio) al di fuori di quanto permesso dalla legge sul copyright
- È proibito copiare in tutto o in parte libri, articoli, rapporti o altri documenti se non per quanto permesso dalla legge sul copyright.

Politica per l'utilizzo di internet, della posta elettronica e sull'uso dei servizi di rete

Nella presente politica si intende regolamentare l'utilizzo di internet e della posta elettronica.

Utilizzo di Internet
Premesso che l'accesso ad internet deve essere utilizzato esclusivamente per finalità lavorative, vale il criterio generale che è proibito l'utilizzo dei servizi di rete per finalità contrarie ai principi etici e morali dell'organizzazione e per finalità per le quali possa essere in qualche modo danneggiata l'immagine aziendale o l'organizzazione stessa.
L'accesso ai servizi di rete è garantito attraverso la rete LAN aziendale.
È proibito collegarsi a reti esterne dai locali aziendali utilizzando collegamenti esterni alla rete aziendale quali ad esempio via modem, tramite la rete fonia di cui è dotato il posto di lavoro se non autorizzati.

È consentito:

- Accedere ai soli siti web autorizzati.

Non è consentito:

- L'accesso a siti dai contenuti non sicuri e in grado di veicolare software malevolo.
- L'accesso a siti dai contenuti contrari ai principi etici e morali dell'organizzazione.
- Violare la sicurezza di archivi e computers della rete.
- Violare la privacy di altri utenti della rete.
- Compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, malware, etc.) costruiti appositamente.

Utilizzo della posta elettronica
Ecco alcune regole cui attenersi per la scrittura dei messaggi:

- Riempire sempre in modo corretto il campo *Da* con il proprio nome e indirizzo e-mail, possibilmente nella forma `nome.cognome@sirfin.it`. Tale campo sarà generato automaticamente una volta configurato correttamente il proprio programma di spedizione.
- Riempire sempre il campo *Oggetto* con una breve descrizione sul contenuto del messaggio.
- Riempire sempre la sezione relativa al corpo del messaggio evitando di utilizzare lettere accentate, tag HTML ed altri caratteri diversi da lettere, numeri e punteggiatura.
- È buona regola spedire i messaggi in formato testo cercando di evitare allegati (Word, immagini o lunghi file di testo):
    - non tutti i programmi di posta riconoscono in modo corretto questi formati;
    - messaggi troppo pesanti (> 10 Mb) possono penalizzare il destinatario con lunghi tempi di attesa durante il recupero dei messaggi.
- Comunque, prima di spedire il messaggio è buona regola comprimere, laddove presenti, gli allegati (*.zip, *.rar, ecc.) e/o trasformarli in formato *.pdf con l'apposito programma (Pdf creator o altri).
- Non spedire mai messaggi di contenuto pubblicitario se non a persone che lo abbiano esplicitamente richiesto.
- Accertarsi che in calce al corpo del messaggio sia presente la propria v-card aziendale e le clausole di riservatezza ai sensi del D.Lgs. 196-03 per il destinatario.
- Se si risponde ad un messaggio, non riportare mai sistematicamente l'intero messaggio originale, se non quando sia necessario, per migliorare la leggibilità ed evitare l'appesantimento del messaggio di risposta.

Regole cui attenersi per i messaggi ricevuti
Organizzare regolarmente i messaggi di posta elettronica come segue:

- Creare cartelle di ricerca che possono essere utilizzate per raggruppare i messaggi per mittente o data o per temi.
- Non aprire mai file sospetti. I file allegati a un messaggio di posta elettronica proveniente da mittente sconosciuto, sospetto o non attendibile, devono essere eliminati senza essere aperti.
- Aprire con accortezza messaggi che contengano in allegato script, eseguibili, link.
- Diffidare dei messaggi contenenti richieste di aiuto, beneficenza o, più in generale, richieste di inoltro ad altre persone o invito a fornire i propri documenti o le proprie credenziali (password): si tratta spesso di fishing.
- Utilizzare un programma antispam impostandone l'elenco dei mittenti bloccati e dei mittenti attendibili oltre che i "settings" di base.

Utilizzo dei servizi di rete
Fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, si sono sviluppati nel corso del tempo una serie di "tradizioni" e di "principi di buon comportamento" che vanno collettivamente sotto il nome di "netiquette" (network etiquette).
Di seguito sono riportati alcuni dei principi fondamentali della "netiquette", a cui tutti sono tenuti ad adeguarsi.

- Quando si aderisce ad un nuovo newsgroup o ad una nuova lista di distribuzione *(mailing list)* via posta elettronica, è bene leggere i messaggi che vi circolano per almeno due settimane prima di inviare propri messaggi in giro per il mondo: in tale modo ci si rende conto dell'argomento e del metodo con cui lo si tratta in tale comunità.
- Se si manda un messaggio, è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema. Specificare sempre, in modo breve e significativo, l'oggetto (campo "Subject") del testo incluso nella mail. Se si utilizza un "signature file", mantenerlo breve e significativo.
- Non divagare rispetto all'argomento del newsgroup o della lista di distribuzione via posta elettronica.
- Evitare, quanto più possibile, broadcast del proprio messaggio verso molte mailing list (o newsgroups). Nella stragrande maggioranza dei casi esiste una ed una sola mailing list che costituisce il destinatario corretto e che include tutti e soli gli utenti che sono effettivamente interessati.
- Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale, se non quando sia necessario.
- Non condurre "guerre di opinione" sulla rete a colpi di messaggi e contromessaggi: se ci sono diatribe personali è meglio risolverle via posta elettronica in corrispondenza privata tra gli interessati.
- Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica.
- Non pubblicare messaggi insignificanti e/o privi di senso o che semplicemente prendono le parti dell'uno o dell'altro fra i contendenti in una discussione. Leggere sempre le FAQ (Frequently Asked Questions) relative all'argomento trattato prima di inviare nuove domande.
- Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state sollecitate in modo esplicito.
- Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

Alle regole precedenti, vanno aggiunti altri criteri che derivano direttamente dal buon senso.
La rete è utilizzata come strumento di lavoro da molti degli utenti. Nessuno di costoro ha tempo per leggere messaggi inutili o frivoli o di carattere personale, e dunque non di interesse generale.
Qualunque attività che appesantisca il traffico o i servizi sulla rete, quali per esempio il trasferimento di archivi voluminosi o l'invio di messaggi di posta elettronica contenenti grossi allegati ad un gran numero di destinatari, deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni in modo da ridurre il più possibile l'impatto sulla rete.

In particolare si raccomanda di:

- effettuare i trasferimenti di archivi in orari diversi da quelli di massima operatività (per esempio in pausa pranzo), tenendo presenti le eventuali differenze di fuso orario;
- non inviare per posta elettronica grosse moli di dati; indicare (ove possibile) la locazione (URL) dei dati nel messaggio, rendendoli disponibili per il prelievo o la consultazione sulla rete.

Vi sono sulla rete una serie di siti server (file server) che contengono, in copia aggiornata, documentazione, software ed altri oggetti disponibili sulla rete. Informarsi preventivamente su quale sia il nodo server più accessibile per l’utente. Se un file è disponibile su di esso o localmente non vi è alcuna ragione per prenderlo dalla rete, impegnando inutilmente la linea e impiegando un tempo sicuramente maggiore per il trasferimento.
Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o re-distribuirlo in qualunque modo e sotto qualunque forma.
Costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge, comportamenti palesemente scorretti da parte di un utente, quali:

- violare la sicurezza di archivi e computers della rete;
- violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;
- compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, malware, etc.) costruiti appositamente.

Politica per l'utilizzo dell'antivirus e delle altre procedure contro il software malevolo

Recenti statistiche relative alla diffusione di software malevolo nei sistemi informativi aziendali riguardanti il tempo medio tra la scoperta di una vulnerabilità software e il suo sfruttamento, la percentuale delle maggiori Aziende mondiali colpite in modo significativo da virus / worm, il numero di nuove vulnerabilità scoperte, la percentuale di tali vulnerabilità considerate facili da sfruttare e la percentuale di tali vulnerabilità considerate altamente pericolose, hanno fatto riflettere la direzione aziendale sulla necessità di dotarsi di adeguate contromisure per fronteggiare efficacemente le nuove minacce.

Quelle che seguono sono alcune delle regole ritenute fondamentali dall'organizzazione per garantire una efficace risposta al problema dei virus informatici.

- Su tutti i PC aziendali deve essere installato un unico programma antivirus *(anche freeware)* dotato di regolare licenza d'uso e del tipo autorizzato dall'Amministratore di Sistema.
- Il programma antivirus dovrà essere interfacciato con il server aziendale preposto allo scaricamento degli aggiornamenti e alla distribuzione a tutti gli utenti.
- Gli utenti dovranno impostare il programma antivirus residente sulla propria macchina in modo da avere gli aggiornamenti in automatico e impostare la pianificazione delle attività di scansione in modo da effettuare almeno una scansione all'avvio del PC e almeno una scansione approfondita nell'arco dell'intera settimana lavorativa.
- Tutti i moduli residenti relativi al programma antivirus dovranno essere impostati sul massimo livello di protezione e in modo da segnalare automaticamente eventuali allarmi a tutti i PC della LAN.
- Non è consentito scaricare e utilizzare altro software antivirus seppure in versione gratuita.
- Su tutti i PC aziendali deve essere installato un unico programma antispamming per la posta elettronica del tipo autorizzato dall'Amministratore di Sistema.
- I filtri relativi a quest'ultimo programma devono essere impostati su livelli appropriati, aggiornandoli attraverso l'apposita area di apprendimento ad ogni operazione di downloading della posta elettronica.

Politica di utilizzo delle Password

Le Password sono un importante aspetto della sicurezza digitale. Sono la prima linea di protezione per gli accessi degli utenti. La scelta di una password "debole" può diventare l'anello debole dell'intera infrastruttura informativa aziendale. Per cui tutti i dipendenti della ARKIVIA PROJECT Srl (inclusi consulenti esterni o agenti) sono responsabili per la corretta applicazione delle linee guida per la scelta e l'archiviazione della password descritte in seguito in questo documento.
L'obiettivo di questa policy è di stabilire degli standard per la creazione di password "forti", la protezione delle password e la frequenza con la quale vengono sostituite.

Regole Generali

- Tutte le password system-level (root, enable, NT admin, application administration accounts, etc.) devono essere cambiate al massimo ogni 3 mesi.
- Tutte le password user-level (email, web, desktop computer, etc.) devono essere cambiate al massimo ogni 6 mesi (l'intervallo consigliato è di 3 mesi).
- Gli account utente che hanno privilegi di sistema devono essere univoche ovvero diverse dalle altre password utilizzate dall'utente.
- Le password non devono mai essere inserite nei messaggi di posta elettronica o in altre forme di comunicazione elettronica.
- Tutte le user-level e system-level password devono essere conformi alle linee guida descritte in seguito.

Linee guida per la scelta della password

Le password, in ARKIVIA PROJECT, vengono utilizzate per differenti finalità.
Alcuni degli utilizzi più comuni sono: user level accounts, web accounts, email accounts, screen saver protection.
Poiché pochi sistemi utilizzano one-time password ogni soggetto interessato deve essere accorto nella scelta delle proprie password.
Password definite "deboli" o "povere" hanno le seguenti caratteristiche:

- La password contiene meno di otto caratteri.
- La password è una parola del dizionario (Italiano o straniero).
- La password è una parola di utilizzo comune come per esempio:
    - Nomi propri di familiari, animali, amici, colleghi, personaggi, etc.
    - Termini e nomi informatici, comandi, siti, società, hardware, software.
    - La parola " ARKIVIA PROJECT", o ogni derivazione
    - Compleanni e altre informazioni personali come indirizzi e numeri di telefono.
    - Pattern di nomi o parole come ad esempio: aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Ciascuna delle precedenti scritta al contrario.
    - Ciascuna delle precedenti seguita o preceduta da una cifra (es., secret1, 1secret)

Le password "forti" hanno le seguenti caratteristiche:

- Contengono lettere upper e lower case (a-z, A-Z).
- Contengono simboli e punteggiatura insieme a lettere: 0-9, !@#$%^&*()_+|~- =\`{}[]:";'<>?,./).
- Sono di almeno 8 caratteri alfanumerici.
- Non sono parole di alcuna lingua, slang, dialetto, etc.
- Non sono basate su informazioni personali, nomi di famiglia, etc.
- Le password non devono mai essere scritte o salvate online. Bisogna cercare di creare password facilmente ricordabili.

Standard di Protezione della Password

Non usare la stessa password per gli account ARKIVIA PROJECT e per altri accessi non relativi al network aziendale (per esempio il collegamento internet personale, l'home banking, etc.). Se possibile non utilizzare la stessa password per differenti accessi ai servizi dei network ARKIVIA PROJECT.

Per esempio, in presenza di reti diverse utilizzare password differenti, scegliere una differente password a seconda della tipologia di sistema utilizzato (Windows/Unix).

Non condividere la password ARKIVIA PROJECT con nessuno inclusi i colleghi e familiari.

Tutte le password devono essere considerate come informazioni sensibili e trattate ai sensi del D.Lgs. 196-03 dalla ARKIVIA PROJECT Srl.

Una lista di cose da NON fare:

- Non comunicare mai la password al telefono a nessuno.
- Non comunicare mai la password in un messaggio email.
- Non comunicare mai la password al superiore.
- Non parlare della password in presenza di più persone.
- Non suggerire mai la password (es. "il nome di un figlio").
- Non comunicare mai password a persone non autorizzate.
- Non comunicare mai la password quando si è in vacanza.

Altre regole:

- Per ogni richiesta di password fare riferimento a questo documento o contattare il Custode delle Password.
- Disabilitare la funzionalità "Ricorda Password" o "Remember Password" (per esempio in: Eudora, OutLook, Netscape Messenger).
- Non trascrivere mai la password su fogli visibili a chiunque. Non salvare mai la password su alcun supporto digitale senza criptarla.
- Cambiare password al massimo ogni 6 mesi (ad eccezione delle system-level password che devono essere cambiate ogni 3 mesi), l'intervallo consigliato è di 3 mesi.
- Se si sospetta che un account o una password siano state diffuse, riportare l'incidente al responsabile diretto provvedendo alla sostituzione immediata.

L'organizzazione si riserva il diritto di ispezionare i sistemi informatici dell'utente per individuare eventuali violazioni di questa policy.

Il dipendente che viola questa policy può essere soggetto ad azione disciplinare.

Politica di clear screen & clear desktop

Quotidianamente, nei locali della sede aziendale, sebbene implementata una procedura per il controllo degli accessi logici e fisici, circola un imprecisato numero di visitatori (clienti, stagisti, fornitori, consulenti, ospiti a vario titolo) che in vario modo possono trovarsi in prossimità delle postazioni di lavoro e venire a contatto con informazioni aziendali più o meno riservate. Al fine di evitare la perdita di confidenzialità ed, eventualmente, la diffusione non autorizzata di tali informazioni, la direzione ha stabilito alcune regole fondamentali cui il personale dipendente deve attenersi.
Quando si abbandona per qualsiasi motivo la postazione di lavoro:

- Assicurarsi che sul PC lasciato incustodito sia attivo lo screen saver con ripristino delle funzionalità esclusivamente attraverso la digitazione della password di screen saver.
- Assicurarsi che nessun dispositivo esterno di memoria sia inserito e/o lasciato incustodito.
- Assicurarsi che eventuale documentazione contenente informazioni ritenute riservate non sia lasciata incustodita sulla scrivania.
- Custodire tale documentazione in armadi o cassettiere munite di serratura.

In presenza di visitatori:

- Non visualizzare sullo schermo del PC files dai contenuti riservati e, eventualmente, provvedere alla loro chiusura o riduzione ad icona.
- Riporre eventuale documentazione contenente informazioni riservate in armadi o cassettiere e, laddove non sia possibile, rendere non visibile il contenuto della stessa documentazione.

Al termine della giornata lavorativa:

- Spegnere il PC ad esclusione dei casi di esecuzione di attività pianificate (ad es. Scansione antivirus) o elaborazioni batch; comunque in tali casi assicurarsi in modo assoluto che il PC sia bloccato.
- Riporre la documentazione contenente informazioni riservate in armadi o cassettiere muniti di serratura e custoditi secondo le stesse modalità di cui sopra.

Politica per l'utilizzo della crittografia
A fine di assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni Arkivia Project prevede l'utilizzo di idonei controlli crittografici. Ove valutato necessario, con idonea analisi dei rischi incombenti sugli asset, sono attuati controlli crittografici per la protezione delle informazioni dalle minacce di violazione della riservatezza e dell'integrità dei dati, anche ai fini di "non ripudio" della autenticità degli stessi.

Si considera la robustezza dell'algoritmo in crittografazione in funzione della criticità dei dati.
La crittografia è valutata come mezzo di protezione delle informazioni memorizzate su dispositivi removibili o apparati mobili di elaborazione. Si valutano inoltre i rischi di impossibilità di "ispezione" di dati cifrati per identificare eventuali "malware".
Sono previste, da parte delle funzioni responsabili degli asset protetti da controlli crittografici, idonee tecniche di protezione e viene stabilita la durata delle chiavi crittografiche attraverso il loro intero ciclo di vita.
Arkivia Project detiene l'elenco dei certificati SSL rilasciati con la validità temporale degli stessi.
Con frequenza almeno trimestrale attraverso personale appositamente incaricato provvede alla verifica di validità degli stessi e, in prossimità della scadenza degli stessi si provvede all'attivazione della procedura di rinnovo.

Sono definiti i metodi di gestione della generazione delle chiavi e delle procedure da adottare in caso di danneggiamento o perdita delle chiavi di decifratura, identificando i responsabili.

In generale, comunque, l'uso della crittografia in Webgenesys è limitata a:

- Le VPN Mobile (SSL VPN)
- la comunicazione HTTPS verso i servizi internet
- l'uso della firma digitale per la firma di documenti.
- La protezione dei dati Backuppati, sia at-rest che in-flight
- Gli accessi SSH, SFTP e SCP a risorse esterne (Offsite) o interne (OnPrem)

Le chiavi crittografiche devono essere generate in modo sicuro e gestite secondo le seguenti linee guida:

- Le chiavi crittografiche devono essere protette da accessi non autorizzati e conservate in luoghi sicuri. A tale scopo vengono usati software come Bitwarden o Keepass, per conservazione in modalità sicura delle Chiavi Crittografiche.
- Le chiavi devono essere generate con lunghezze adeguate e periodicamente cambiate.
- Devono essere mantenute copie di backup delle chiavi crittografiche in caso di perdita o guasto. Le Chiavi registrate su Keepass sono conservate su un Database protetto da password; il DB risiede su un Drive di Google, ed è soggetto a policy di backup automatiche. Le chiavi registrate su Bitwarden, vengo memorizzate su un DB all'interno della VM che ospita l'applicativo. La VM Bitwarden viene regolarmente sottoposta a backup.

L'accesso alle chiavi crittografiche e ai dati crittografati è consentito solo al personale autorizzato in base alle necessità di lavoro. L'autorizzazione è soggetta a workflow documentato.
Questa politica viene sottoposta a revisione periodica per assicurare l'adeguatezza e l'efficacia in risposta alle minacce in evoluzione.

Creazione di un accont su AWS intestato ad Arkivia Project, creazione delle nuove chiavi crittografiche e accesso all'accont profilato per mansione aziendale (Le chiavi le genera Danilo e le vedono Davide e Rocco e possono anche gestirle Davide e Rocco); Inoltre per i certificati SSL, Davide verifica trimestralmente la validità dei certificati e il loro aggiornamento
Certificati SSL: 1

Politica per la Regolamentazione della contrattualistica con terze parti

Negli accordi con terze parti, per soddisfare i requisiti identificati per la sicurezza, devono essere presi in considerazione alcuni, a seconda della tipologia di contratto, tra i seguenti aspetti:

- La politica per la sicurezza delle informazioni.
- I controlli per garantire la protezione dei beni (p.es. protezione di software e informazioni, protezioni fisiche, protezione contro software malevoli, verifiche di eventuali perdite o modifiche delle informazioni, di software, di hardware; assicurare la restituzione o la distruzione di informazioni e di beni alla fine del contratto o in un momento concordato; riservatezza, integrità, disponibilità e ogni altra pertinente proprietà dei beni; restrizioni sulla copiatura e la divulgazione delle informazioni e uso di accordi di riservatezza).
- L'informazione su metodi e procedure inerenti la sicurezza.
- La sensibilizzazione degli utenti relativamente alle responsabilità e alle questioni inerenti la sicurezza delle informazioni.
- Le responsabilità riguardanti installazione e manutenzione di hardware e software.
- La politica per il controllo accessi (requisiti, benefici e ragioni che rendano necessario l'accesso della terza parte; metodi di accesso consentiti e il controllo e l'uso di identificativi unici come *user ID* e *password*).
- Le disposizioni per dare evidenza di eventuali incidenti inerenti la sicurezza delle informazioni e delle relative violazioni.
- Le rispettive responsabilità delle parti nell'accordo.
- Le responsabilità su aspetti legali (p.e. la legislazione sulla protezione dei dati).
- I diritti di proprietà intellettuale e assegnazione del copyright anche nel caso di lavori effettuati in collaborazione.
- Il coinvolgimento della terza parte con subappaltatori e i controlli per la sicurezza che devono essere attuati da tali subappaltatori.

Politica per il trasporto in sicurezza delle informazioni su supporto cartaceo

Occasionalmente, in Arkivia, si presenta l'evenienza di dover trasferire materialità o documenti su supporto cartaceo da e verso i clienti con personale proprio.
Per soddisfare i requisiti di integrità, disponibilità e riservatezza dei dati e delle informazioni trasportate, il personale si impegna a prelevare la materialità e il supporto su cui le informazioni e i dati sono contenuti senza alterarne gli imballi o i sigilli eventualmente apposti e a consegnarli tal quali al destinatario.
Nel contempo sia Arkivia che il cliente si impegnano a presentare alla persona incaricata del trasporto, le materialità o i supporti in formato non accessibile all'incaricato.

Politica per l’esecuzione dei backup.

In considerazione del fatto che i dati presenti sulle singole macchine e sui server aziendali costituiscono il patrimonio informativo fondamentale per l’azienda è opportuno effettuare i backup di tali informazioni tenendo conto anche di quanto riportato nelle istruzioni operative cui si fa esplicito rimando.