Cyber Security Policy

Clean desk....3
Sicurezza dei dispositivi informatici....5
Uso delle password....7
Linee guida per la creazione delle password....9
Posta elettronica....11
Installazione di programmi....13
Uso consentito delle risorse informatiche....14
Accesso da remoto....16
Programmi per l'accesso da remoto....18
Collegamento wireless....20
Standard per le comunicazioni wireless....22
Dismissione di apparecchiature....24
Sicurezza per i Server....26
Sicurezza dei laboratori didattici....27
Log....29
Risposta ad un Data Breach....31
Dispositivi informatici Bluetooth....33
Cifratura dei dati....35
Supporti di memorizzazione portatili....37
Backup....38

Clean desk

Panoramica

La politica di *Clean desk* è uno strumento importante per garantire che tutti i documenti o dispositivi informatici contenenti dati personali siano rimossi dall'area di lavoro dell'Incaricato al trattamento e siano messi sottochiave quando non sono in uso o quando l'Incaricato lascia la sua postazione di lavoro.

È una delle prime accortezze da utilizzare quando si vuole ridurre il rischio di violazioni della sicurezza sul posto di lavoro.

Scopo

Lo scopo di questa policy è quello di stabilire i requisiti minimi per il mantenimento di un *Clean desk* in modo che i dati personali degli studenti, dei genitori, del personale scolastico, dei fornitori siano messi al sicuro.

La *Clean desk* non è solo conforme allo standard ISO 27001/17799, ma fa anche parte dei controlli standard effettuati per verificare la corretta applicazione dei requisiti relativi al GDPR.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Policy

1. Gli utenti sono tenuti a garantire che tutte le informazioni personali, siano esse in forma cartacea o digitale, siano inaccessibili alla fine dell'orario di lavoro o nel caso in cui si dovesse lasciare il posto di lavoro per un periodo di tempo prolungato.
2. I dispositivi informatici devono essere bloccati quando non si è alla propria scrivania.
3. I dispositivi informatici devono essere completamente spenti alla fine della giornata lavorativa.
4. Tutte le informazioni personali devono essere rimosse dalla scrivania e poste sottochiave al termine della giornata lavorativa.
5. Gli schedari contenenti informazioni personali devono essere tenuti chiusi a chiave quando non sono in uso o quando non si è fisicamente presenti nella stanza.
6. Le chiavi utilizzate per aprire gli schedari contenenti informazioni personali non devono essere lasciate incustodite.
7. I portatili devono essere fissati con un cavo di bloccaggio al fine di impedirne il furto.
8. Le password non possono essere riportate su post-it né possono essere scritte in posti accessibili.
9. Le stampe effettuate ed i fax ricevuti, contenenti dati personali, devono essere immediatamente rimossi dal vassoio di stampa.
10. Al momento dello smaltimento, i documenti contenenti dati personali devono essere passati al distruggidocumenti
11. Le lavagne contenenti informazioni personali devono essere cancellate.
12. Quando non in uso, tenere sottochiave i dispositivi informatici portatili come laptop e tablet.

13. Trattare i dispositivi informatici di archiviazione di massa, quali unità CDROM, DVD o USB, come contenenti informazioni sensibili e tenerli sottochiave.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone.

Sicurezza dei dispositivi informatici

Panoramica

Mantenere sicuri i dispositivi informatici assegnati è essenziale per garantire che non ci siano accessi non autorizzati ai dati trattati dall'Istituto.

Scopo

Lo scopo di questa policy è quello di fornire indicazioni su come garantire la sicurezza delle informazioni presenti all'interno dei propri dispositivi informatici e a quelli a cui si ha accesso da tali dispositivi informatici.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi che accedono con computer propri o forniti dall'Istituto alla rete dell'Istituto.

Policy

Per impedire accessi, modifiche o cancellazioni indebite da parte di persone non autorizzate al trattamento di dati personali devono essere prese delle misure appropriate.

1. L'accesso fisico ai dispositivi informatici deve essere limitato ai soli autorizzati.
2. Gli utenti, prima di abbandonare la propria postazione di lavoro, devono attivare sui propri dispositivi informatici il salva schermo o devono effettuare la disconnessione così che sia necessario reimmettere la password prima di poter accedere.
3. Deve essere impostare l'avvio del salva schermo dopo pochi minuti di inattività con la richiesta della password.
4. Gli utenti devono assicurarsi che i dispositivi informatici siano utilizzati solo per attività lavorative.
5. Gli utenti non devono installare programmi non autorizzati.
6. Gli utenti devono memorizzare tutte le informazioni sensibili solo all'interno di server così da semplificarne la protezione.
7. Gli utenti non devono consumare bevande o cibo vicino ai dispositivi informatici così da evitare accidentali cadute di liquidi che possono danneggiarli.
8. I portatili che contengono informazioni personali devono essere bloccati fisicamente alla scrivania con un cavo di acciaio o devono essere tenuti sottochiave quando non in uso.
9. Sui portatili deve essere implementata la cifratura del disco.
10. Il Sistema Operativo deve essere mantenuto aggiornato alle ultime patch e, quando non più supportato dal fornitore, deve essere aggiornato alla versione successiva.
11. I programmi installati non più in uso devono essere rimossi, così come i loro dati.
12. Se la posizione dello schermo permette di sbirciare quello che viene mostrato sul video, installare un filtro polarizzato che restringe il campo di visione allo stretto necessario o utilizzare altre cortine per celare le informazioni personali.
13. Prima di abbandonare i dispositivi informatici, chiudere tutti i documenti ed uscire da tutte le applicazioni.

14. Utilizzare uno scaricatore di sovratensioni o un gruppo di continuità per proteggere i dispositivi informatici da sbalzi di corrente.
15. Se viene utilizzato un accesso wireless alla rete dell'Istituto, seguire le indicazioni riportate nella policy *Collegamento wireless*.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Uso delle password*, *Linee guida per la creazione delle password*, *Cifratura dei dati*, *Collegamento wireless*.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, ecc.

Uso delle password

Panoramica

Le password sono un aspetto importante della sicurezza del computer.

Una password scelta male può comportare l'accesso non autorizzato e/o lo sfruttamento delle risorse dell'Istituto scolastico.

Scopo

Lo scopo di questo criterio è quello di stabilire uno standard per l'uso di password complesse e la protezione di tali password.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Policy

Creazione di password

1. Tutte le password a livello di utente e di sistema devono essere conformi alla policy *Linee guida per la creazione delle password*.
2. Gli utenti devono utilizzare una password univoca separata per ciascuno dei loro account relativi al lavoro.
3. Gli utenti non possono utilizzare le password relative all'attività lavorativa per i propri account personali.
4. Gli account utente che dispongono di privilegi a livello di sistema concessi tramite appartenenze a gruppi o programmi come sudo, devono avere una password diversa da quella di tutti gli altri account detenuti da tale utente.
   Inoltre, si consiglia vivamente che una qualche forma di autenticazione a più fattori venga utilizzata per tutti gli account con privilegi elevati.

Cambio di password

1. Le password devono essere modificate solo quando vi è motivo di credere che una password sia stata compromessa.
2. Per verificare la bontà della password scelta, può essere eseguito da parte dell'Istituto un tentativo di scoprirla utilizzando idonei programmi di cracking.
   Se una password viene scoperta durante uno di questi controlli, l'utente dovrà cambiarla seguendo le linee guida indicate nella policy *Linee guida per la creazione delle password.*

Custodia della password

1. Le password non devono essere condivise con nessuno, inclusi supervisori e colleghi. Tutte le password devono essere considerate come informazioni riservate.
2. Le password non devono essere inserite nei messaggi e-mail, nei programmi di messaggistica o in altre forme di comunicazione elettronica, né rivelate al telefono.
3. Le password possono essere archiviate solo in "gestori di password" autorizzati dall'Istituto scolastico.

4. Non utilizzare la funzione "Memorizza password" delle applicazioni (ad esempio, i browser web).
5. Se si sospetta che la propria password sia stata compromessa, si deve immediatamente segnalare l'incidente al proprio Responsabile e si devono modificare tutte le password in proprio possesso.

Procedure

Le procedure in uso devono implementare le seguenti misure di sicurezza:

1. Devono supportare l'autenticazione del singolo utente e non di un gruppo.
2. Non devono memorizzare le password in chiaro o in una forma facilmente reversibile.
3. Non devono trasmettere le password in chiaro sulla rete.
4. Devono prevedere una qualche forma di trasferimento dei ruoli così che un utente possa svolgere le funzioni di un altro utente senza aver bisogno di conoscerne la password.

Autenticazione MFA

1. L'autenticazione multifattoriale è fortemente consigliata e dovrebbe essere utilizzata per tutti gli account lavorativi.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi che valutano la robustezza delle password, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy*: Linee guida per la creazione delle password*.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Linee guida per la creazione delle password

Panoramica

Le password sono una componente fondamentale della sicurezza delle informazioni.

Le password servono per proteggere l'account dell'utente; tuttavia, una password mal costruita, può comportare la compromissione di sistemi, dati o rete.

Scopo

Lo scopo di questa linea guida è quello di fornire le migliori indicazioni per la creazione di password robuste.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Queste linee guida si applicano a tutte le password quali, a titolo esemplificativo ma non esaustivo, account a livello di utente, account a livello di sistema, account Web, account e-mail, protezione dello screen saver, segreteria telefonica e accessi router locali.

Policy

Robustezza della password

- Maggiore è il numero di caratteri utilizzati, maggiore è la robustezza della password. Si consiglia un minimo di 14 caratteri nella password.
- Per la creazione delle password si consiglia l'uso di frasi – password costituite da più parole – quali, ad esempio: "Tempo di vacanza" o "Blocco-curioso-sole-foglie". Le passphrase sono facili da ricordare e digitare e soddisfano i requisiti di resistenza all'attacco.

Password non accettabili

- Contengono 8 caratteri o meno.
- Contengono informazioni personali quali date di nascita, indirizzi, numeri di telefono, nomi di familiari, di animali domestici o di personaggi dello spettacolo.
- Contengono ripetizioni di caratteri come aaabbb, qwerty, zutsrq, or 123321.
- Sono del tipo di "Benvenuto123", "Password123" "Cambiami123".

Per consentire agli utenti di gestire agevolmente più password, si consiglia l'uso di un programma di "Gestione delle password" che sia autorizzato e fornito dall'Istituto scolastico.

Si consiglia inoltre, ogni volta sia possibile, di abilitare l'uso dell'autenticazione a più fattori.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi che valutano la robustezza delle password, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Posta elettronica

Panoramica

La posta elettronica viene utilizzata in modo pervasivo in tutti i settori ed è spesso il metodo di comunicazione più usato.

Allo stesso tempo, l'uso improprio delle e-mail, può rappresentare un rischio dal punto di vista normativo, di privacy e di sicurezza, quindi è importante che gli utenti facciano un uso appropriato delle comunicazioni elettroniche.

Scopo

Lo scopo di questa policy è quello di garantire un uso appropriato del sistema di posta elettronica e rendere edotti gli utenti di quali comportamenti sono considerati accettabile e di quali sono considerati inappropriati.

Quelli indicati sono i requisiti minimi per un corretto utilizzo della posta elettronica dell'Istituto.

Ambito di applicazione

Queste linee guida illustrano l'uso corretto del sistema di posta elettronica e si applicano al personale scolastico e a tutti i fornitori, consulenti, lavoratori temporanei e altri lavoratori che operano per conto dell'Istituto.

Policy

1. Tutti gli utilizzi della posta elettronica devono essere coerenti con le politiche dell'Istituto e con le procedure di condotta etica, sicurezza e conformità alle leggi applicabili.
2. L'account di posta elettronica dell'Istituto deve essere utilizzato solo per le comunicazioni relative all'attività lavorativa.
3. I dati personali contenuti nel messaggio e negli eventuali allegati devono essere protetti con metodi di cifratura secondo quanto indicato dal GDPR.
4. I messaggi di posta elettronica devono essere conservati solo se contengono informazioni relative all'attività lavorativa.
5. La conservazione dei messaggi deve essere effettuata secondo le regole previste dall'Istituto.
6. Il sistema di posta elettronica dell'Istituto non deve essere utilizzato per scopi ricreativi o per distribuire messaggi inappropriati o offensivi quali, a titolo esemplificativo ma non esaustivo, commenti offensivi su razza, sesso, disabilità, età, orientamento sessuale, pornografia, credenze e pratiche religiose, appartenenza politica o origine razziale.
   Il personale che dovesse ricevere messaggi di tale natura ne deve dare immediata notizia al suo Responsabile.
7. Agli utenti non è consentito inoltrare automaticamente i messaggi di posta elettronica a un sistema di posta elettronica di terze parti.
   I singoli messaggi inoltrati dall'utente non devono contenere informazioni personali.

8. Agli utenti non è consentito utilizzare in ambito lavorativo sistemi di posta elettronica di terze parti diversi da quelli istituzionali fornito dall'Istituto o utilizzare sistemi di memorizzazione quali Google Drive, dropbox e similari.
9. Gli utenti non devono aspettarsi alcuna privacy per i messaggi che ricevono od inviano utilizzando il sistema di posta elettronica istituzionale.
10. L'istituto può monitorare, senza preavviso, lo scambio di e-mail effettuato in ambito lavorativo.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi di monitoraggio dei messaggi scambiati audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Installazione di programmi

Panoramica

Permettere agli utenti l'installazione autonoma di programmi espone l'Istituto ad un rischio non necessario.

I problemi più comuni che possono verificarsi quando gli utenti installano programmi non autorizzati comprendono: l'installazione di versioni non compatibili di DLL che impediscono ad alcuni programmi di funzionare; l'introduzione di malware; l'installazione di programmi privi di licenza che espongono il Titolare a responsabilità amministrative e/o penali; l'installazione di programmi che compromettono la sicurezza della rete.

Scopo

Lo scopo di questa policy è quello di indicare i requisiti che devono essere soddisfatti prima di poter installare programmi sul proprio Pc.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Questa policy riguarda tutti i dispositivi informatici installati nell'Istituto.

Policy

1. Gli utenti non possono installare programmi nei dispositivi informatici connessi alla rete dell'Istituto.
2. I programmi necessari per poter eseguire i compiti assegnati devono essere approvati da un Responsabile prima di poter essere installati.
3. I programmi da installare devono essere reperiti, direttamente o tramite i consulenti/fornitori dell'Istituto, solo da canali certificati ed approvati da un Responsabile.
4. Il Responsabile deve tenere traccia delle licenze acquistate e verificare che quanto installato non superi quanto acquistato.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi di monitoraggio dei programmi installati e del numero di licenze acquistate ed usate, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, ecc.

Uso consentito delle risorse informatiche

Panoramica

Le risorse informatiche a disposizione quali, a titolo esemplificativo ma non esaustivo, programmi, dispositivi informatici, posta elettronica, credenziali di accesso alle procedure, ecc. sono di proprietà dell'Istituto e devono essere usate per svolgere i compiti assegnati e null'altro, ciò al fine di proteggere, anche dal punto di vista economico, l'Istituto.

Mantenere la sicurezza dell'ambiente informatico è compito di tutti e gli utenti hanno la responsabilità di seguire questa e le altre policy così da garantire il corretto trattamento delle informazioni personali.

Scopo

Lo scopo di questa policy è quello di definire quale è l'uso consentito delle risorse informatiche dell'Istituto così da proteggere gli utenti e l'Istituto da azioni di rivalsa da parte di terzi dovute a mancato rispetto della normativa.
Un uso inappropriato delle risorse informatiche espone l'Istituto al rischio di attacchi hacker, malware, compromissione della rete e dei servizi erogati e ad azioni legali.

Ambito di applicazione

Queste linee guida si applicano all'uso di informazioni, apparecchiature informatiche e risorse di rete da parte del personale scolastico, dei fornitori, dei consulenti, dei lavoratori temporanei e di altri lavoratori, compreso tutto il personale affiliato a terzi.

Policy

1. Le informazioni contenute nelle risorse informatiche dell'Istituto sono di sua proprietà e devono essere trattate in ottemperanza alle policy, alle leggi e ai regolamenti.
2. Ogni incidente che fa temere la perdita, il furto, l'accesso illecito, la modifica illecita deve essere immediatamente riferito al Responsabile.
3. Le informazioni trattate dall'Istituto possono essere condivise solo nell'ambito della propria attività lavorativa e solo con terze parti autorizzate.
4. L'attività di rete e dei dispositivi informatici può essere controllata in ogni momento al fine di ottimizzarne le prestazioni, di controllarne la sicurezza e per effettuare operazioni di manutenzione.
5. L'Istituto si riserva il diritto di effettuare periodicamente degli audit per verificare che questa e le altre policy siano correttamente applicate.
6. Non devono essere collegate alla rete dell'Istituto dispositivi informatici propri senza essere stati prima autorizzati dal Responsabile.
7. Le credenziali di accesso (nome utente e password) ricevute per operare con le procedure dell'Istituto non devono essere scambiate con altri né devono essere custodite in modo non sicuro così da permetterne l'accesso ad alcuno.
8. È vietato violare il diritto di copyright installando programmi di cui l'Istituto non ha regolare licenza.
9. È vietata la copia non autorizzata di materiale protetto da copyright quale, a titolo esemplificativo ma non esaustivo, libri, musica, foto, video, ecc.

10. È vietato l'accesso a dati, programmi o server dell'Istituto al difuori di quanto strettamente necessario per lo svolgimento del proprio lavoro, anche se si hanno le credenziali per poterlo fare.
11. È vietato installare programmi malevoli all'interno della rete dell'Istituto quali, a titolo esemplificativo ma non esaustivo, virus, scanner, worm, trojan, ecc.
12. È vietato rivelare le credenziali assegnate dall'Istituto ad altri o a familiari e conviventi in caso di lavoro da casa.
13. È vietato compromettere il regolare funzionamento della rete dell'Istituto o tentare di superare le misure di sicurezza effettuando operazioni quali, a titolo esemplificativo ma non esaustivo, scaricare video o musica, tentare di accedere a server o risorse a cui non si ha diritto, effettuare lo sniffing del traffico di rete, effettuare attacchi di tipo DOS, fare post scanning, superare le procedure di autenticazione e autorizzazione in essere, ecc.
14. È vietato fornire informazioni sulla configurazione, tipologia e misure di sicurezza in atto nella rete dell'Istituto.
15. È vietato utilizzare la rete dell'Istituto per effettuare comunicazioni, via e-mail o social media, non richieste (spam), di minaccia, provocatorie, ecc.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, ecc.

Accesso da remoto

Panoramica

L'accesso da remoto alla rete dell'Istituto può essere essenziale per mantenere la produttività, ma, in alcuni casi, l'accesso avviene da reti che possono essere state compromesse o che hanno un livello di sicurezza significativamente inferiore rispetto a quello dell'Istituto.

Poiché queste reti sono al difuori del controllo diretto da parte dell'Istituto è necessario definire delle policy che possano ridurre al massimo tali rischi.

Scopo

Lo scopo di questa policy è quello di definire regole e presupposti per la connessione alla rete dell'Istituto da parte di dispositivi informatici esterni.

Le regole sono pensate per minimizzare l'esposizione dell'Istituto ai danni che possono derivare da un accesso non autorizzato alle risorse interne.

I danni possono riguardare il furto di dati personali, danno all'immagine dell'Istituto, danni alle apparecchiature, e multe o altre perdite finanziarie legate ad accessi illeciti.

Ambito di applicazione

Questa policy si applicano al personale scolastico e a tutti i fornitori, consulenti, lavoratori temporanei e altri lavoratori che operano per conto dell'Istituto che utilizzano un computer proprio o di proprietà dell'Istituto per connettersi alla rete dell'Istituto.

Questa policy si applica alle connessioni remote stabilite per attività lavorative effettuate per conto dell'Istituto.

Questa policy copre tutte le prescrizioni tecniche che devono essere seguite per potersi collegare da remoto alla rete dell'Istituto.

Policy

È responsabilità del personale scolastico, dei fornitori, dei consulenti, dei lavoratori temporanei e degli altri lavoratori che operano per conto dell'Istituto garantire che all'accesso remoto vengano applicate tutte le policy e le accortezze previste dal lavoro in presenza.

Quando si opera da remoto è obbligatorio impedire l'accesso alle risorse o ai dati dell'Istituto a persone non autorizzate.

Sono vietate attività illegali effettuate utilizzando la rete dell'Istituto e chi accede da remoto è responsabile e risponde di attività improprie.

Non è permesso l'accesso ad internet al difuori di quanto necessario per l'esecuzione dei propri compiti.

Requisiti

1. L'accesso da remoto deve essere permesso solo mediante canali cifrati, per esempio VPN, e mediante l'utilizzo di password forti.
   Per ulteriori informazioni, consultare le policy *Uso delle password*, *Linee guida per la creazione delle password*.
2. Gli utenti che accedono da remoto devono proteggere le loro credenziali, anche dai propri familiari.
3. Gli utenti devono assicurarsi che durante il lavoro da remoto il computer utilizzato non sia connesso a nessun'altra rete, a parte quella dell'Istituto, con l'eccezione di reti dichiarate affidabili dal Responsabile o sotto il completo controllo dell'utente.
4. L'uso di risorse esterne deve essere approvato anticipatamente da parte del Responsabile.
5. Tutti dispositivi informatici che si collegano da remoto alla rete dell'Istituto devono aver installato un programma antivirus aggiornato.
6. Nel caso in cui per l'accesso remoto vengano utilizzato apparecchiature non dell'Istituto, la configurazione hardware e software di tali computer deve essere approvata da un Responsabile.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi di monitoraggio dei programmi installati e del numero di licenze acquistate ed usate, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Uso delle password*, *Linee guida per la creazione delle password*.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, ecc.

Programmi per l'accesso da remoto

Panoramica

I programmi per l'accesso remoto permettono ad un utente o a un addetto al supporto tecnico di condividere lo schermo e le risorse del computer senza la necessità della presenza in loco.

Alcuni di tali programmi sono TeamViewer, AnyDesk, Supremo e il Desktop remoto di Windows.

Mentre tali programmi possono far risparmiare molto tempo eliminando la necessità di spostamenti e permettono la collaborazione di più utenti, creano anche un punto di entrata alla rete dell'Istituto che può essere utilizzata per il furto, la modifica e la distruzione di informazioni personali.

Per questo motivo l'utilizzo di tali programmi deve essere preventivamente approvato da un Responsabile.

Scopo

Questa policy definisce le caratteristiche che devono avere i programmi utilizzati per l'accesso remoto.

Ambito di applicazione

Questa policy si applica a tutte le comunicazioni, in entrata ed in uscita, che interessano un server o un Pc dell'Istituto.

Policy

Tutti gli strumenti utilizzati per collegare macchine dell'Istituto con l'esterno devono essere in linea con i seguenti requisiti.

L'Istituto mette a disposizione sistemi per la collaborazione tra risorse interne ed esterne.

La lista di programmi approvati è a disposizione presso il Responsabile che fornirà anche istruzioni sulla corretta installazione e configurazione per ognuno di essi in modo da garantire la sicurezza delle comunicazioni.

Requisiti

1. Tutti i sistemi di accesso alla rete interna dell'Istituto devono prevedere una autenticazione multifattoriale prima che sia possibile accedere alle risorse interne. Ad esempio l'accesso dall'esterno con Desktop remoto mediante una VPN filtrata da un firewall, che accetta solo quel tipo di connessione, necessita di una prima password per accedere al certificato digitale (qualcosa che ho) così da poter stabilire la VPN e di una successiva password (qualcosa che so) per l'autenticazione al dominio.
2. Il database utilizzato per l'autenticazione deve essere Active Directory o LDAP ed il protocollo utilizzato deve essere cifrato e non suscettibile al replay attack.
3. Il canale utilizzato per stabilire la connessione deve utilizzare meccanismi di cifratura forte.

4. L'antivirus e tutti i meccanismi di sicurezza predisposti dall'Istituto non devono essere disabilitati, by-passati o modificati in alcun modo.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi di monitoraggio dei programmi installati e del numero di licenze acquistate ed usate, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Uso delle password* e *Linee guida per la creazione delle password*.

Definizioni e termini

Nessuno.

Collegamento wireless

Panoramica

La massiccia adozione di smartphone, tablet e portatili ha portato all'implementazione di accessi wireless in ogni organizzazione.

Una configurazione non adeguata di tali accessi può fornire un semplice canale di accesso a malintenzionati.

Scopo

Lo scopo di questa policy è quello di mettere al sicuro e proteggere le informazioni trattate dall'Istituto.

Vengono indicate le precondizioni che l'infrastruttura wireless deve avere prima di poter concedere l'accesso alla rete dell'Istituto.

Solo i dispositivi informatici che aderiscono a questa policy possono essere utilizzati per connettersi.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Si applica a tutti i dispositivi che forniscono l'accesso alla rete dell'Istituto e a tutti i dispositivi informatici.

Sono comprese tutte le forme di comunicazione wireless.

Policy

Tutti i dispositivi informatici wireless che fanno parte dell'infrastruttura di rete dell'Istituto o che forniscono accesso alle informazioni personali trattate dall'Istituto devono:

1. Essere conformi a quanto indicato nella policy *Standard per le comunicazioni wireless*.
2. Essere installati e supportati da personale interno o esterno selezionato dal Responsabile.
3. Avere un MAC address immodificabile.
4. Non interferire tra di loro.

I dispositivi informatici wireless dei laboratori didattici devono:

1. Essere isolati fisicamente o logicamente (firewall) dalla rete principale a cui sono collegate i dispositivi informatici contenenti dati personali.
2. Non interferire con la rete principale.

I dispositivi informatici wireless della rete casalinga a cui è collegato un dispositivo utilizzato per l'accesso remoto devono:

1. Essere conformi a quanto dettagliato nella policy *Standard per le comunicazioni wireless*.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi di monitoraggio, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Sicurezza dei laboratori didattici, Standard per le comunicazioni wireless*.

Definizioni e termini

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, stampanti, ecc.

Standard per le comunicazioni wireless

Panoramica

I collegamenti wireless rappresentano un punto di accesso privilegiato per i malintenzionati poiché possono essere sfruttati anche da lontano, mediante l'utilizzo di apposite antenne che ne estendono il raggio di azione ben oltre i confini dell'Istituto.

È quindi necessario applicare tutte le accortezze disponibili per evitare l'accesso, la modifica o la distruzione di informazioni personali trattate dall'Istituto.

Scopo

Questa policy specifica quali sono le caratteristiche tecniche che devono avere le apparecchiature che si collegano in modalità wireless alla rete dell'Istituto.

Le apparecchiature in esame includono dispositivi informatici quali, a titolo esemplificativo ma non esaustivo, switch, firewall, dispositivi informatici per l'accesso remoto, modem, access point.

Per l'infrastruttura dei laboratori didattici deve essere applicato quanto riportato nella policy *Sicurezza dei laboratori didattici*.

Ambito di applicazione

Tutto il personale scolastico, i fornitori, i consulenti, i lavoratori temporanei e gli altri lavoratori, compreso tutto il personale affiliato a terzi che gestisce l'infrastruttura wireless per conto dell'Istituto deve seguire quanto indicato in questa policy.

Policy

Tutti i dispositivi informatici che si collegano alla rete dell'Istituto o che fornisco accesso a tale rete devono aderire ai seguenti standard:

1. Usare per l'autenticazione il protocollo EAP-FAST, il protocollo PEAP o EAP-TLS.
2. Usare il protocollo TKIP o la cifratura AES con una lunghezza minima della chiave di 128 bit.
3. Tutti i dispositivi informatici Bluetooth devono usare il Secure Simple Pairing con la cifratura abilitata.

Per i laboratori didattici il SSID deve essere diverso da quello della rete principale e non ne deve essere effettuato il broadcast.

Tutti i dispositivi informatici che si collegano all'infrastruttura casalinga di utenti che effettuano l'accesso remoto alla rete dell'Istituto devono:

1. Abilitare l'accesso mediante WPA-PSK, EAP-FAST, PEAP o EAP-TLS.
2. Quando si utilizza WPA-PSK, la password deve essere di almeno 20 caratteri.
3. Deve essere disabilitato il broadcast del SSID.
4. Deve essere cambiato il SSID preimpostato dalla fabbrica.
5. Devono essere cambiate le credenziali preimpostate in fabbrica sull'access point.

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi di monitoraggio, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Sicurezza dei laboratori didattici*.

Definizioni e termini

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Access point, Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, stampanti, ecc.

Dismissione di apparecchiature

Panoramica

Le apparecchiature informatiche contengono parti che non possono essere semplicemente conferite all'indifferenziata.

Il riciclaggio è una responsabilità ecologica ed è previsto dalla legge.

Inoltre, dischi, chiavette USB, CD-ROM ed altri dispositivi di memorizzazione possono contenere informazioni personali dell'Istituto.

Per proteggere le informazioni affidate dagli Interessati al Titolare del trattamento, tutti i dispositivi di memorizzazione devono essere cancellati in modo adeguato prima di procedere al loro riciclaggio.

La semplice cancellazione o la formattazione dei dispositivi non è considerata sufficiente.

Quando si procede alla cancellazione o anche alla formattazione di un dispositivo, i dati vengono segnati come cancellati, ma rimangono ancora disponibili fino a quando non vengono sovrascritti da nuove informazioni.

Quindi bisogna utilizzare programmi appositi che effettuano cancellazioni sicure prima di procedere alla dismissione dei dispositivi.

Scopo

Lo scopo di questa policy è quello di fornire indicazioni su come procedere alla dismissione di apparecchiature di proprietà dell'Istituto.

Ambito di applicazione

Questa policy si applica a tutte le apparecchiature o dispositivi di memorizzazione che non sono più necessari all'Istituto quali, a titolo esemplificativo ma non esaustivo, Pc, server, dischi, portatili, smartphone, tablet, periferiche (tastiere, mouse, altoparlanti), stampanti, scanner, dispositivi di memorizzazione esterna, nastri di backup.

Tutto il personale scolastico deve applicare questa policy.

Policy

1. Quando i dispositivi informatici sono giunti al termine della loro vita utile devono essere riciclati in modo opportuno sotto la supervisione di un Responsabile.
2. Il Responsabile si preoccuperà di cancellare in modo sicuro ed irreversibile tutte le informazioni contenute nelle apparecchiature da dismettere.
3. Le licenze software, eventualmente presenti, dovranno essere recuperate così da poter essere installate su nuove apparecchiature.
4. La vendita di apparecchiature, in alternativa al riciclaggio, deve essere approvata da un Responsabile.
5. Nessuna apparecchiatura deve essere conferita all'indifferenziata, ma deve essere avviata al riciclaggio.
6. Il Responsabile provvederà a cancellare i dati contenuti nei nastri, nei dischi, nelle schede SD, nelle chiavette USB, ecc. o a sovrascriverne i dati con programmi appositi.

In alternativa alla cancellazione, i dispositivi di memorizzazione devono essere resi inutilizzabili con metodi fisici (schiacciamento, foratura o altri metodi di demolizione). I dispositivi ottici (CD-ROM, DVD, WORM, ecc.),devono essere fisicamente distrutti.

7. Con il termine apparecchiature si intendono, a titolo esemplificativo ma non esaustivo: desktop, portatili, tablet, server, stampanti, fotocopiatrici, telefoni, smartphone, switch, router, access point, nastri di backup, dischi esterni, chiavette USB, batterie, ecc.
8. Il Responsabile della cancellazione dei dati rendiconterà l'avvenuta cancellazione indicando la data in cui è avvenuta, il metodo utilizzato e la persona/ditta esterna che ha provveduto all'operazione.
9. Per le apparecchiature non funzionanti, i dispositivi informatici di memorizzazioni devono essere rimossi e distrutti fisicamente.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Nessuno.

Sicurezza per i Server

Panoramica

Server vulnerabili e non sicuri sono il principale punto di ingresso per gli hacker.
Una valida politica di installazione, configurazione, manutenzione e gestione dei server è quindi di fondamentale importanza.

Scopo

Lo scopo di questa policy è quello di definire i requisiti minimi di installazione e configurazione per i server utilizzati dall'Istituto.

L'implementazione attenta di questa policy minimizza il rischio di accessi non autorizzato alle informazioni personali trattate dall'Istituto.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

La policy si applica a tutti i server di proprietà o utilizzati dall'Istituto all'interno della propria rete.

Policy

1. Tutti i server in esercizio presso l'Istituto devono essere assegnati ad un Responsabile che, direttamente o tramite fornitori esterni, ne cura l'amministrazione.
2. Tutti i server sono inventariati e la loro configurazione, i dati contenuti ed i programmi installati devono essere comunicati al Titolare.
3. Il Sistema Operativo dei server deve essere mantenuto aggiornato alle ultime patch e, quando non più supportato dal fornitore, deve essere aggiornato alla versione successiva.
4. I programmi installati non più in uso devono essere rimossi dal server, così come i loro dati.
5. Per operare su di un server utilizzare sempre un account con i minimi privilegi amministrativi sufficienti per effettuare il lavoro.
6. I server devono essere ospitati in stanze in cui l'accesso è controllato e non in aree pubbliche.
7. Nel sistema operativo dei server devono essere abilitati i log per tutti gli eventi relativi alla sicurezza.
8. Il server deve essere sottoposto a backup periodico sia della configurazione che dei programmi e dei dati degli applicativi installati così da essere in linea con le policy di RTO – Recovery Time Objective – e RPO – Recovery Point Objective – definite per i dati trattati.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Nessuno.

Sicurezza dei laboratori didattici

Panoramica

La contemporanea presenza di reti dedicate alla didattica e alla gestione dell'Istituto non deve costituire una fonte di rischio per i dati personali affidati al Titolare del trattamento.

È quindi necessario adottare misure opportune per garantire una completa separazione dei due ambiti.

Scopo

Lo scopo di questa policy è quello di definire le regole che è necessario adottare per salvaguardare le risorse dei laboratori didattici e per salvaguardare la rete dell'Istituto da rischi che possono derivare da macchine non protette o da accessi non autorizzati provenienti dalla rete dei laboratori didattici.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Queste linee guida si applicano a tutte le macchine destinate ai laboratori didattici anche se poste al difuori della rete locale dell'Istituto.

Policy

1. Deve essere nominato un Gestore dei laboratori didattici.
2. Il Gestore è responsabile della sicurezza dei laboratori e deve badare che i laboratori non abbiano alcun impatto sulla sicurezza della rete dell'Istituto e sulle sue prestazioni.
3. Il Gestore è responsabile dell'applicazione alla rete dei laboratori di tutte le policy di sicurezza dell'Istituto.

4. Il Gestore è responsabile dell'accesso fisico alle apparecchiature dei laboratori.
5. Tutte le password utilizzate nei laboratori devono aderire alle relative policy dell'Istituto.
6. Le credenziali non più in uso devono essere cancellate entro tre giorni dal momento in cui l'utente non è più autorizzato all'accesso alle risorse dei laboratori.
7. I personal computer dei laboratori devono avere antivirus approvati dal Responsabile, tali antivirus devono essere tenuti aggiornati e devono effettuare una scansione periodica.
   Macchine eventualmente infettate da malware devono essere scollegate dalla rete dei laboratori fino a quando non è stato rimosso ogni malware.
8. Devono essere seguite le indicazioni contenute nella policy *Uso accettabile* e quindi sono proibite tutte le attività malevoli quali la distribuzione di virus, spam, trojan, ecc.
9. Nessuna macchina dei laboratori può ospitare programmi utilizzati per la gestione dell'Istituto.
10. Le macchine dei laboratori non devono contenere dati personali.
11. Tutto il traffico generato dai laboratori deve passare per un firewall che lo separa completamente dalla rete dell'Istituto.
12. I dispositivi di rete dei laboratori non devono essere interconnessi direttamente con la rete dell'Istituto, ciò vale anche per eventuali apparati wireless.
13. Il Responsabile può interrompere l'operatività dei laboratori nel caso in cui essi presentino rischi o causino degrado delle prestazioni alla rete dell'Istituto.
14. Una eventuale connessione autonoma ad internet per la rete dei laboratori deve essere autorizzata da un Responsabile che provvederà ad effettuare un attento esame dell'impatto che può avere in termini di sicurezza.
15. Le password utilizzate nelle apparecchiature di rete dei laboratori devono essere diverse da quelle utilizzate all'interno della rete dell'Istituto.
    Le password devono essere create ed utilizzate in linea con le policy dell'Istituto.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Nessuno.

Log

Panoramica

La registrazione delle attività effettuate nei sistemi critici per le informazioni trattate può fornire indicazioni fondamentali ed indicare se ci sono state compromissioni della sicurezza o se è in atto un attacco.

Anche se i log non vengono esaminati quotidianamente, è importante averli così da poter effettuare un'analisi a posteriore in caso di Data Breach.

Scopo

Lo scopo di questa policy è quello di identificare le caratteristiche che devono avere i programmi e i sistemi in uso nell'Istituto per poter generare log utili e completi.

In caso di acquisizione di nuove procedure, dovrà essere posta attenzione alle funzioni di log messe a disposizione e alle modalità di attivazioni di tale prestazione.

Ambito di applicazione

Queste linee guida si applicano a tutte le procedure e apparecchiature in esercizio nell'Istituto.

Policy

Tutti i sistemi che trattano informazioni personali, che accettano connessioni di rete o controllano l'accesso, cioè svolgono compiti di autenticazione ed autorizzazione, devono generare e memorizzare log contenenti informazioni sufficienti a rispondere ai seguenti quesiti:

1. Quale attività è stata svolta?
2. Chi o cosa ha svolto tale attività e da quale sistema?
3. Su cosa è stata svolta l'attività?
4. Quando è stata svolta l'attività?
5. Con quale strumento è stata svolta l'attività?
6. L'attività è stata portata a termine?
7. Quale è stato il risultato dell'attività?

Quindi devono essere generati log ogni volta che:

1. Si creano, leggono, modificano o cancellano informazioni critiche, incluse quelle relative alla modifica delle credenziali di accesso.
2. Viene tentato un acceso alla rete.
3. Viene effettuato un accesso alla rete.
4. Viene autenticato un utente.
5. Vengono modificate le autorizzazioni di un utente o di un gruppo.
6. Viene cambiata la configurazione del firewall, dell'antivirus o di altri strumenti deputati alla sicurezza della rete.
7. Viene cambiata la configurazione di sistemi, della rete o delle procedure, includendo l'installazione di patch o di aggiornamenti.
8. Viene effettuato il riavvio di server, procedure, sistemi.

9. I programmi applicativi o di sistema o i servizi di sistema si arrestano in modo inaspettato.
10. Le risorse dei server (CPU, memoria, dischi, rete, ecc.) si saturano.

Tali log devono contenere informazioni che permettono, come minimo, di identificare, direttamente o indirettamente:

1. Il tipo di azione effettuata, ad esempio: autenticazione, autorizzazione all'accesso, alla creazione, alla lettura, all'aggiornamento e alla cancellazione.
2. Il nome del sottosistema che effettua l'azione, ad esempio: processo, identificativo della transazione.
3. Identificativo dell'utente che richiede l'azione, ad esempio: nome utente, nome del computer, indirizzo IP, MAC address.
4. Identificativo dell'oggetto su cui viene svolta l'azione, ad esempio: nome del file, identificativo del record e nome della tabella del database, nome del computer, indirizzo IP, MAC address.
5. Se possibile, il valore prima e dopo la modifica dell'oggetto trattato.
6. Data ed ora in cui l'azione è stata effettuata.
7. Se l'azione era permessa o meno.
8. Indicazione del motivo per cui un'azione è stata rifiutata.

Il sistema deve supportare una forma di registrazione dei log che ne garantisca la non modificabilità e l'autenticità.

Il formato dei log deve essere, se possibile, standard così da facilitarne l'analisi con strumenti automatizzati.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Risposta ad un Data Breach

Panoramica

Il Regolamento Europeo 2016/679 – GDPR – definisce il "Data Breach" come una 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.

Compito del Titolare del trattamento è impedire una violazione della sicurezza che può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Scopo

Lo scopo di questa policy è quello di definire i passi da intraprendere nel caso si sospetti o si abbia la certezza che si sia verificato un Data Breach, così da mettere l'Istituto in grado di rispondere alla violazione della sicurezza nel modo più appropriato ed in linea con le disposizioni di legge.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi e si applicano ai dati personali così come definiti dal Regolamento Europeo 2016/679.

Policy

1. Chiunque venisse a conoscenza, direttamente o indirettamente, di un possibile Data Breach ne deve dare immediata comunicazione al proprio Responsabile, che provvederà ad informare il Titolare del trattamento, o direttamente al Titolare del trattamento.
2. Il Titolare del trattamento facendosi coadiuvare, se necessario, dal personale deputato al trattamento dei dati in oggetto e da personale tecnico interno e/o esterno provvederà a:
    a. Sospendere immediatamente il trattamento dei dati di cui si ipotizza il Data Breach.
    b. Informare il DPO del possibile Data Breach così da farsi aiutare nell'indagine volta a confermare o smentire l'evento.
    c. Mettere sottochiave i documenti cartacei che riguardano i dati di cui si ipotizza il Data Breach al fine di permettere un'adeguata indagine.
    d. Spegnere e porre sotto custodia le macchine contenenti i dati di cui si ipotizza il Data Breach al fine di permettere un'adeguata indagine.
    e. Avviare una verifica per confermare o meno il Data Breach.
    f. Documentare l'incidente per eventuali revisioni a posteriori delle politiche di sicurezza dell'Istituto.

Se il Data Breach dovesse essere confermato, il Titolare del trattamento, facendosi coadiuvare dal DPO, provvederà a:

g. Informare il Garante della Privacy e, se necessario, l'Autorità Giudiziaria.
h. Se richiesto dal Regolamento Europeo 2016/679, ad informare gli Interessati.

i. Prendere tutte le azioni necessarie (formazione del personale, aumento delle misure di sicurezza fisiche, aumento delle misure di sicurezza informatiche, revisione delle policy, ecc.) volte ad impedire il ripetersi del Data Breach.

Se il Data Breach non è avvenuto, ma nell'indagine effettuata sono emerse criticità nella sicurezza, il Titolare prenderà spunto dall'evento per potenziare le misure di sicurezza in essere.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Nessuna.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

DPO: Data Protection Officer, in italiano il Responsabile della Protezione Dati.

Dispositivi informatici Bluetooth

Panoramica

I dispositivi informatici Bluetooth sono sempre più presenti all'interno degli Istituti.

La portata di tali dispositivi informatici è in costante crescita e connessioni Bluetooth insicure possono rappresentare un rischio per la rete dell'Istituto.

Scopo

Lo scopo di questa policy è quello di definire gli standard minimi di sicurezza a cui devono rispondere i dispositivi informatici prima di permetterne il collegamento ai dispositivi informatici della rete dell'Istituto così da salvaguardare i dati personali trattati.

Ambito di applicazione

Queste linee guida si applicano a tutti i dispositivi informatici Bluetooth che si collegano ai dispositivi informatici dell'Istituto.

Policy

Versione

Non può essere utilizzato alcun dispositivo che non rispetti lo standard Bluetooth 2.1 o successivi.

PIN e Pairing

- Non effettuare il pairing tra i dispositivi informatici Bluetooth in aree pubbliche dove il PIN può essere illecitamente acquisito.
- Se, dopo aver effettuato il pairing, viene nuovamente richiesto il PIN, non inserirlo nuovamente perché è possibile che stiano tentando di acquisirlo illecitamente, pertanto è opportuno rivolgersi ad un Responsabile per segnalare l'incidente.

Impostazioni dei dispositivi informatici

- Tutti i dispositivi informatici Bluetooth devono essere impostati per la "sicurezza modo 3" in modo che venga cifrato il traffico in ambedue le direzioni.
- Usare un PIN lungo almeno 8.
- Impostare il dispositivo Bluetooth in modalità nascosta così che non renda nota la sua presenza.
- Attivare il Bluetooth solo quando necessario.
- Mantenere aggiornati i dispositivi informatici all'ultima versione del firmware.

Uso non consentito

Non è possibile utilizzare dispositivi informatici Bluetooth per:

- Captare trasmissioni altrui, effettuare l'impersonificazione di dispositivi informatici altrui, impedire l'uso di dispositivi informatici altrui o ogni altra tipologia di attacco.
- Usare dispositivi informatici Bluetooth dell'Istituto con dispositivi informatici non dell'Istituto.

Responsabilità dell'utente

- È compito dell'utente rispettare questa policy.

- I dispositivi informatici Bluetooth devono essere spenti quando non in uso.
- Dati personali non devono essere trasmessi o memorizzati mediante dispositivi informatici Bluetooth.
- Devono essere utilizzati solo ed esclusivamente dispositivi informatici Bluetooth approvati dall'Istituto.
- I PIN e la configurazione dei dispositivi informatici Bluetooth devono essere mantenuti riservati dall'utente.
- Ogni incidente di sicurezza o uso improprio di dispositivi informatici Bluetooth deve essere immediatamente riferita al Responsabile.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Definizioni e termini

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Access point, Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, stampanti, ecc.

Cifratura dei dati

Panoramica

Uno dei metodi che si hanno a disposizione per proteggere dati personali residenti su memorie di massa è la cifratura che rende i dati inaccessibili a chi non ha a disposizione la password necessaria a decifrarli.

È possibile cifrare i dati direttamente nel momento in cui si effettua il salvataggio del documento che si vuole proteggere altrimenti è possibile creare una cartella in cui tutti i dati contenuti vengono automaticamente cifrati oppure cifrare un intero disco sia esso fisico o logico.

Scopo

Lo scopo di questa policy è quello di definire i criteri di applicazione della cifratura dei dati.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

La policy si applica a tutti i dati personali trattati all'interno dell'Istituto.

Policy

1. I dati personali trattati all'interno dell'Istituto devono essere memorizzati, e sottoposti a backup, in forma cifrata.
2. È compito del Responsabile del trattamento stabilire, di volta in volta, se ricorrere alla cifratura a livello di sistema, che interessa tutto il disco (ad esempio utilizzando la funzione BitLocker disponibile in Windows 10 o equivalenti sistemi per macchine Linux), oppure se definire una cartella riservata o anche ricorrere alla cifratura documento per documento.
3. Gli utenti sono tenuti ad osservare le indicazioni fornite dal Responsabile.
4. La password utilizzata per cifrare deve essere conservata con la massima attenzione e deve rispondere alle indicazioni contenute nelle policy *Uso delle password* e *Linee guida per la creazione delle password*.
5. L'utente deve essere consapevole che la perdita della password comporta la perdita definitiva dei dati cifrati.
6. Per comunicare la password a terzi – Responsabili esterni del trattamento – deve essere utilizzato un canale di comunicazione diverso da quello utilizzato per lo scambio di dati.
   Ad esempio, se si trasmette via e-mail un documento cifrato, la password necessaria a decifrarlo deve essere comunicata via telefono, SMS, Whatsapp, ecc. ma non via e-mail.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: U*so delle password*, *Linee guida per la creazione della password*.

Definizioni e termini

Per Utente si intende, a titolo esemplificativo ma non esaustivo: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Supporti di memorizzazione portatili

Panoramica

Lo smarrimento o il furto di dispositivi di memorizzazione portatili (dischi esterni, chiavette USB, schede SD, dischi contenuti nei laptop, memoria di smartphone e di tablet) contenenti dati personali comporta un Data Breach e può comportare un notevole danno per l'Istituto.

Scopo

Lo scopo di questa policy è quello di definire i criteri di utilizzo dei dispositivi informatici di memorizzazione portatili.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

La policy si applica a tutti i dati personali trattati all'interno dell'Istituto.

Policy

1. L'uso di dispositivi di memorizzazione portatili deve essere riservata a casi particolari, essere occasionale ed essere preventivamente autorizzata dal Responsabile.
2. Il dispositivo deve essere cifrato, seguendo le indicazioni contenute nella policy *Cifratura dei* dati, così da rendere minimo l'impatto del Data Breach in caso di furto o smarrimento.
3. Gli utenti sono tenuti ad osservare le indicazioni fornite dal Responsabile.
4. Ove sia necessario accedere a dati personali da dispositivi informatici diversi da quelli di lavoro, sono da privilegiare soluzioni quali la condivisione via cloud, ad esempio G-Suite (purché sia attiva una autenticazione a più fattori) oppure una VPN.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Cifratura dei* dati.

Definizioni e termini

Utenti: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, ecc.

Backup

Panoramica

Il backup dei dati personali è l'unico strumento in grado di recuperare dati andati persi, modificati per errore o oggetto di attacco hacker o virus quali CryptoLocker.

Scopo

Lo scopo di questa policy è quello di definire i criteri di backup.

Ambito di applicazione

Queste linee guida si applicano al personale scolastico, ai fornitori, ai consulenti, ai lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

La policy si applica a tutti i dati personali trattati all'interno dell'Istituto.

Policy

1. Il backup deve essere cifrato per evitare che un suo accesso illecito provochi un Data Breach.
2. Devono essere sottoposti a backup tutti i dati personali.
3. Gli utenti che devono necessariamente conservare dati personali all'interno dei loro dispositivi informatici devono darne comunicazione al Responsabile che provvederà ad attivarne il backup.
4. Per i server, oltre al backup dei dati, va presa in esame l'ipotesi di sottoporre a backup anche la configurazione del Sistema Operativo e delle procedure così da facilitarne il ripristino in caso se ne renda necessaria la sostituzione o la reinstallazione ex-novo.
5. Deve essere sottoposta a backup anche la configurazione delle apparecchiature di rete quali firewall, router, access point, ecc.
6. Nel caso in cui i dati siano affidati a servizi Cloud, va verificata la presenza del backup, la sua retention e le metodologie di ripristino.
7. Per ogni tipologia di dati è compito del Responsabile stabilire la retention del backup.
8. Periodicamente deve essere effettuato un ripristino dei dati su di un dispositivo di lavoro per verifica che il backup sia leggibile, che contenga tutte le informazioni, che le procedure di ripristino siano efficienti e ben documentate, che i tempi di ripristino siano compatibili con l'operatività dell'Istituto.
9. È consigliabile effettuare i backup su due supporti diversi quali ad esempio Cloud e disco/NAS/nastro locale, al fine di avere una separazione fisica tra i backup e garantire la possibilità di ripristino anche in caso di problemi in uno dei due backup.

Conformità

Verifica della conformità

Il Responsabile verifica il rispetto di questa policy utilizzando vari metodi che includono, ma non sono limitati a: la verifica di persona, l'uso di programmi appositi, audit interni ed esterni e riscontro da parte del personale scolastico.

Eccezioni

Ogni eccezione a questa policy deve essere precedentemente autorizzata da un Responsabile.

Non conformità

La violazione di questa policy può portare a procedimenti disciplinari.

Standard, Policy e Processi correlati

Regolamento europeo 2016/679 – GDPR.

Policy: *Cifratura dei* dati.

Definizioni e termini

Utenti: personale scolastico, fornitori, consulenti, lavoratori temporanei e ad altri lavoratori, compreso tutto il personale affiliato a terzi.

Per Dispositivo informatico si intende, a titolo esemplificativo ma non esaustivo: Server, Pc, laptop, tablet, smartphone, memorie di massa esterne, ecc.