Istituto Tecnico
Fossati - Da Passano
La Spezia

ISTITUTO TECNICO COMMERCIALE E TECNOLOGICO "Agostino FOSSATI - Manfredo DA PASSANO"

Sede Centrale: Via Bragarina, 32/A - 19126 - La Spezia -Telefono 0187 500557
Sede staccata: Via Caranza, 32 - 19028 - Varese Ligure (SP) - Telefono 0187 842171
Sito: www.fossatidapassano.it **Mail**: sptd110005@istruzione.it **Pec**: sptd110005@pec.istruzione.it

Regolamento Privacy

Trattamento dei Dati

REGISTRAZIONE DELLE EDIZIONI

Edizione	Data	Descrizione delle modifiche introdotte
01	10-10-2022	Prima edizione

INDICE

1. INTRODUZIONE

Il presente Regolamento in materia di protezione dei dati personali (cosiddetta 'Privacy') è uno strumento di applicazione del **Regolamento Europeo n. 2016/679 (General Data Protection Regulation - GDPR).**

Il presente documento definisce:

- un insieme di regole e di politiche per la gestione della Privacy, atte a consentire la gestione sicura dei dati elettronici e cartacei;
- un insieme di processi operativi che utilizzano correttamente le regole e le politiche descritte e ne consentono il miglioramento continuo.

Le politiche e le regole sono adottate da parte dell'ITCT Fossati-Da Passano La Spezia (di seguito l'Istituto).

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

2. PERIMETRO DI VALIDITÀ

Le regole e le politiche definite in questo documento si applicano a tutte le sedi, le persone dell'Istituto e agli asset che contengono dati personali (elettronici o cartacei) in esse contenuti. Il personale, i consulenti e le terze parti dell'Istituto sono tenuti ad attenersi a tali regole e politiche.

3. RIFERIMENTI

UNI EN ISO 9000:2015	Sistemi di gestione per la qualità - Fondamenti e Vocabolario
UNI EN ISO 9001:2015	Sistemi di gestione per la qualità - Requisiti
DLgs 196/2003 ITA	D. Lgs 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali (Privacy), allegato B al medesimo e successivi provvedimenti del Garante sulla Privacy (in Italia);
GDPR	Regolamento 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ed il DLgs 196/2003 (regolamento generale sulla protezione dei dati)
ISO/IEC 27001:2017	Information Security Management Systems – Requirements
Working Party	Gruppo di lavoro europeo sulla Privacy

4. DEFINIZIONI E ACRONIMI

Definizione	Descrizione
Autorità di Controllo:	Autorità di Controllo: Autorità pubblica incaricate di sorvegliare l'applicazione del GDPR (Garante Privacy)
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ('Interessato'); con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni al suo stato di salute
Trattamento (dati)	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Titolare Legale	Titolare Legale: Il rappresentate legale
Titolare del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento dei dati personali
Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta o sotto la cui responsabilità e controllo vengono trattati dati personali per conto del Titolare.
Interessati	Le persone fisiche identificate o identificabili alle quali sono riferiti i dati personali
Incaricati	Dipendenti o qualsiasi altra persona fisica autorizzata a compiere operazioni di Trattamento dei Dati

	Personali da parte dell'Istituto e/o dai propri eventuali Subresponsabili Rientrano in questa categoria anche il Titolare ed i Responsabili quando essi eseguono Trattamenti
Amministratori di Sistema o AdS	Dipendenti o qualsiasi altra persona fisica autorizzata a compiere operazioni di accesso o modifica dei Dati Personali da parte dell'Istituto e/o dai propri eventuali Subresponsabili, agendo direttamente sui sistemi informatici
Misure di Sicurezza	Le misure di sicurezza previste ai sensi della Normativa Privacy e ogni altro obbligo previsto ai sensi della Normativa Privacy al fine di garantire la sicurezza e la riservatezza dei Dati Personali, ivi comprese le attività da compiere in caso di Violazione dei Dati Personali;
Data Protection Officer o DPO o RPD	Responsabile della Protezione dei Dati. Persona fisica con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati, designato dall'Istituto
Sub-responsabile	Persona giuridica, ditta individuale o libero professionista incaricato da un fornitore (Responsabile esterno) di eseguire, per conto di esso, le attività che comportano il Trattamento dei dati personali
Personal Computer (PC)	Computer personale dedicato ed utilizzato da una singola persona
Rete DMZ	DeMilitarizedZone, porzione di rete dati esposta su internet (rete pubblica)
Data-at-Rest	Dato stabile nel sistema, memorizzato all'interno di Banche Dati o sistemi di storage
Remote Access	Tecnologia che permette l'accesso remoto (esterno) alle reti dati (es. Virtual Private Network Remote Access)
Banca Dati	Contenitori di dati personali elettronici o cartacei
STI	Supporto tecnico informatico, servizio che gestisce l'infrastruttura informatica
BYOD	Bring your device – utilizzo per motivi lavorativi del proprio device (apparato) per connettersi alla rete dell'Istituto

5. ORGANIZZAZIONE PRIVACY

Di seguito sono descritti i ruoli (e le loro responsabilità) che intervengono nel processo di gestione della privacy per l'Istituto.

5.1 Titolare del Trattamento

Il Titolare del Trattamento è il Titolare Legale o, eventualmente, un suo delegato.

Il Titolare del Trattamento determina le finalità dei trattamenti dei dati impegnandosi ad effettuare trattamenti in conformità al presente regolamento ed in modo lecito, corretto e trasparente nei confronti degli Interessati.

Il Titolare del Trattamento garantisce nei confronti degli Interessati, che:

- I Trattamenti effettuati siano conformi alle finalità dichiarate;
- Le finalità dichiarate siano limitate a quanto necessario per l'esercizio dell'attività istituzionali;
- Vengano utilizzati solo i dati necessari per le finalità dichiarate;
- La conservazione dei dati sia limitata nel tempo ad un periodo congrui con le finalità dichiarate;
- Siano implementati sistemi atti a garantire la conservazione dei dati,
- Per ogni Trattamento sia verificato il criterio di legittimità dello stesso;
- Le informative rilasciate agli Interessati siano corrette e conformi a quelle previste nella gestione dei Trattamenti.

Inoltre, il Titolare provvede:

- a nominare con atto deliberativo, laddove ritenuto opportuno o laddove necessario, i Responsabili del Trattamento dei dati personali (interni o esterni), impartendo loro, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli Interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'Interessato all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
- a nominare il Data Protection Officer (DPO)
- a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati.

5.2 Responsabile del Trattamento

Gli eventuali Responsabili del Trattamento (interni ed esterni) nominati dal Titolare devono:

- garantire che le persone autorizzate al trattamento dei dati personali siano a conoscenza e vincolate a obblighi di riservatezza in relazione ai Dati che si trovano a trattare;
- coadiuvare il Titolare nella mappatura dei trattamenti e nella redazione del Registro dei Trattamenti;
- adottare le misure di sicurezza previste
- assistere il Titolare segnalando la necessità di adottare misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di evadere le richieste degli Interessati di cancellare, modificare o restituire tutti i dati personali;
- provvedere alla cancellazione o restituzione dei dati personali esaurita la finalità per cui sono stati raccolti e trattati

5.3 Data Protection Officer (DPO)

Il DPO svolge l'attività consulenziale di supervisore indipendente, a favore del Titolare e dei Responsabili e dietro loro richiesta.
Inoltre il DPO:

- Collabora con il Titolare e con i Responsabili per le richieste degli Interessati;
- Si occupa di monitorare l'evoluzione della normativa e dei provvedimenti delle Autorità di Controllo e aggiornare Titolare e Responsabili ove questi possano avere un impatto sui trattamenti di cui al Registro dei Trattamenti;
- Coordina le attività di mantenimento del Registro dei Trattamenti e di gestione dei rischi effettuate dal Titolare (ed eventuali Responsabili interni) incoraggiando un uniforme e adeguato livello di sicurezza nel trattamento dei dati personali;
- Con cadenza almeno annuale, promuove e coordina con il Titolare una revisione dei contenuti delle politiche per la gestione dei trattamenti, del Registro dei Trattamenti e supporta il Titolare nella definizione di piani di miglioramento;
- Assiste il Titolare nell'erogare una appropriata formazione in materia di protezione dei dati al personale che ha accesso ad essi permanente o regolare;
- Riceve (dal Titolare o dai Responsabili) le richieste degli Interessanti e li assiste nell'evasione di tali richieste;
- E' il punto di contatto con le Autorità di Controllo, assistendo il Titolare nelle relazioni con le Autorità;
- Ha accesso garantito alla documentazione necessaria alla comprensione dei trattamenti di dati personali;

- Produce e condivide relazioni, , laddove necessario, sulle attività connesse al trattamento dei dati personali, alle attività del DPO e alle attività necessarie per la compliance con il GDPR.

6. PROCESSI PRIVACY

6.1 Informativa

Il Titolare, in caso di raccolta di dati personali di un Interessato, fornisce all'Interessato, nel momento in cui i dati personali sono ottenuti, la corretta informativa sulle modalità del trattamento degli stessi.

L'informativa può essere rilasciata secondo il modello 'M1-Informativa' o tramite un formato che contenga un sottoinsieme sufficiente agli scopi delle informazioni previste nel citato modello.

6.2 Consenso

Il Titolare assume che ogni trattamento deve trovare fondamento in base giuridica (consenso, adempimento obblighi contrattuali, interessi vitali della persona Interessata o di terzi, obblighi di legge cui è soggetto l'Istituto, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente).

La richiesta di consenso può essere fatta tramite sottoscrizione del modello 'M1-Informativa e Consenso' da parte dell'Interessato, o tramite un formato che contenga un sottoinsieme sufficiente agli scopi delle informazioni previste nel citato modello.

6.3 Procedura di Gestione delle Richieste degli Interessati

Il Titolare tutela i diritti degli Interessati consentendo:

- accesso ai dati personali;
- diritto di limitazione al Trattamento
- diritto di opposizione;
- diritto di rettifica;
- richiesta di revoca del consenso;
- diritto di cancellazione (oblio);
- diritto al trasporto (portabilità) dei dati personali.

Il Titolare è il destinatario ultimo delle richieste formulate dagli Interessati, che possono essere veicolate in vari modi (casella di posta del DPO; mail dirette al Titolare e ai Responsabili, varie forme comunicative, comunicazione alla Segreteria). Coloro che ricevono tali istanze le comunicano prontamente al Titolare.

Il DPO, su ingaggio del Titolare, coadiuva il Titolare nell'esame delle richieste ricevute, nelle azioni necessarie all'evasione della richiesta e nel riscontro all'Interessato.

6.3.1 Portabilità dei dati personali

Tutte le Banche Dati utilizzate sono esportabili in formati standard, corredate dove necessario dai tracciati dei record e leggibili da parte di esperti terzi, in modo da garantire la portabilità, in caso di emergenza, dei dati all'esterno del sistema informatico.

6.3.2 Cancellazione dei dati personali (diritto all'Oblio)

La cancellazione dei dati personali avviene tramite opportuni strumenti software messi a disposizione dai sistemi o dagli applicativi e garantisce la possibilità di cancellare anche solamente parti di dati delle Banche Dati trattate.

Laddove si intende trattenere i dati personali (es. a fini statistici) oltre il periodo temporale di conservazione consentito si usa l'anonimizzazione degli stessi. Più in generale l'anonimizzazione è sempre possibile come alternativa alla cancellazione.

I dati personali (di produzione o di collaudo o di test) contenuti nelle banche dati gestite dall'Istituto (dati interni dell'Istituto) sono conservati:

motivatamente, tutto il tempo necessario per espletare le attività dell'Istituto;

in modo da poter sempre ottemperare agli adempimenti previsti dalla legge vigente;

L'Istituto, in caso di dati personali affidati e trattati da terzi, specifica il tempo di conservazione degli stessi, nel rispetto delle regole di cui sopra. In caso non sia esplicitamente specificato il tempo di conservazione è da intendersi coincidente con tutto il tempo di durata dell'attività.

Gli applicativi utilizzati garantiscono il 'diritto all'oblio' agli Interessati, cioè consentono la cancellazione totale e puntuale dei dati personali del singolo Interessato. Qualora sia esercitato il diritto all'oblio da parte di un Interessato, esso è espletato se e solo se tale richiesta non confligge con eventuali obblighi di natura giuridica o lede il legittimo interesse dell'Istituto.

Le tempistiche di cancellazione dei dati sono specificate nel Registro dei Trattamenti.

6.4 Registro dei Trattamenti

Il Titolare ed i Responsabili provvedono, al fine di garantire completezza delle informazioni mappate e uniformità di analisi, a tracciare i Trattamenti effettuati mediante la realizzazione del Registro Trattamenti (compilato per ciascuna area di competenza in cui viene suddivisa l'organizzazione, con indicazione di ciascun Trattamento effettuato all'interno di tale area).

Si adotta il modello 'R6-Registro Trattamenti'.

6.5 Valutazione dei Rischi e degli Impatti nel Trattamento dei dati personali

Il Titolare (coadiuvato dal DPO) provvede alla valutazione dei rischi per i casi di violazione dei dati personali e all'identificazione delle misure di miglioramento per abbattere i rischi alle soglie di tollerabilità.

Nell'analisi dei rischi sono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutate le possibili conseguenze. Gli eventi presi in considerazione rientrano nelle seguenti categorie:

Comportamenti degli Incaricati: tutti gli scenari in cui il comportamento maldestro o fraudolento di un Incaricato può provocare un problema di sicurezza dei dati personali;

Eventi relativi agli strumenti: tutti gli scenari in cui un problema ad uno dei sistemi informatici dell'infrastruttura informatica può provocare un problema di sicurezza dei dati personali;

Eventi relativi al contesto fisico-ambientale: tutti gli scenari in cui, indipendentemente dal comportamento degli operatori e dal corretto funzionamento dei sistemi, si possono comunque concretizzare problemi per la sicurezza dei dati personali.

La valutazione del rischio è calcolata su scala a cinque valori (molto alto/alto/medio/basso/molto basso) come prodotto di tre componenti:

La gravità (impatto) del danno o della minaccia che si potrebbe verificare;

La vulnerabilità dell'asset;

La stima della probabilità che il danno o la minaccia si verifichino.

La valutazione della necessità di Valutazione d'Impatto sulla Protezione dei Dati Personali (DPIA) è calcolata su scala a cinque valori (molto alto/alto/medio/basso/molto basso) come identificazione dei tipi di dati personali trattati e della quantità della loro presenza secondo i criteri indicati dal Working Party Privacy europeo. Tale valore è poi messo a prodotto con i valori calcolati per l'AR in forma matriciale.

In caso si renda necessario, il Titolare esegue DPIA, Valutazione dell'Impatto sul Trasferimento dei Dati Personali (TIA) o altre valutazioni di rischio e di impatto che ritiene idonee e/o necessarie.

A seguito di queste analisi, per tutti gli indicatori che riportano un rischio alto. è prodotto un piano di rimedio in cui sono identificate le misure di sicurezza da adottare per abbattere i rischi.

6.6 Formazione e Sensibilizzazione

L'Istituto sostiene e promuove, al suo interno, ogni strumento di formazione e sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale (effettuata su base annuale) e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Istituto.

Per garantire la conoscenza capillare delle disposizioni introdotte dal GDPR, al momento dell'ingresso in servizio è fornita, a cura della Segreteria, ad ogni dipendente o collaboratore una specifica comunicazione in materia di Privacy, con apposita clausola inserita nel contratto di lavoro (lettera di nomina a persona autorizzata).

6.7 Processo di Revisione delle Credenziali e dei Profili

Il possesso delle credenziali e dei diritti (profilatura) sono verificati (revisionati) con cadenza almeno annuale da parte del DPO. Il processo prevede che il DPO riceve le liste delle credenziali e dei profili associati dal STI e verifica la correttezza e l'attualità degli stessi. Nei casi in cui il DPO rileva incongruenze o diritti non più validi, procede a comunicarlo al STI affinché provveda a configurare correttamente e conseguentemente le credenziali ed i profili sui computer, sugli applicativi e sui sistemi.

6.8 Procedura di Notifica in Caso di Violazione dei Dati (Data Breach)

Con il termine Data Breach si intende un incidente di sicurezza in cui dati personali sono consultati, copiati, trasmessi, rubati, utilizzati da un soggetto non autorizzato, distrutti o persi. Il Data Breach si realizza in seguito a:

- Perdita accidentale;
- Distruzione non recuperabile;
- Furto;
- Divulgazione non consentita;
- Accesso abusivo.

Chiunque (all'interno dell'Istituto) abbia motivo di ritenere che vi sia stata una violazione dei dati personali trattati, ha l'obbligo di informare immediatamente il Titolare e/o, se presente il Responsabile, su tale evento (specifica formazione sul punto verrà erogata a favore di tutti gli autorizzati al trattamento).

Ricevuta la segnalazione il Titolare e/o il Responsabile provvedono a coinvolge il DPO allo scopo di essere supportati nella disamina dell'evento e nella eventuale notifica all'Autorità di Controllo.

Il DPO verifica gli eventi e le modalità del sospetto Data Breach, ed in caso sia accertato il caso di Data Breach, provvede ad eseguire le seguenti attività, in collaborazione con il STI e con il personale dell'Istituto:

- ripristino delle condizioni di corretto funzionamento;
- analisi delle cause che hanno prodotto il Data Breach ed eventuale correzione o mitigazione delle vulnerabilità rilevate.

Il Titolare provvede alla notifica all'Autorità di Controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento dell'accertamento e, laddove necessario, alla comunicazione agli Interessati.

La notifica all'Autorità di Controllo contiene:

- La descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- La comunicazione del nome e i dati di contatto del DPO e/o di altro punto di contatto presso cui ottenere più informazioni;
- La descrizione delle probabili conseguenze della violazione e delle misure adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire le informazioni contestualmente alla notifica è formulata riserva di successiva integrazione.

Il Titolare del Trattamento mantiene un registro delle violazioni occorse nel formato 'R2-Registro Data Breach'.

6.9 Comunicazione dati personali verso l'Esterno

La comunicazione di dati personali da parte dell'Istituto verso un altro soggetto pubblico o privato è ammessa quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.

7. BYOD

Gli apparati personali (PC, mobile, smartphone o similari) per essere collegati alla rete dell'Istituto devono essere verificati ed autorizzati da STI.

Gli apparati sono autorizzati se:

- Nell'apparato è installato Software supportato e con le corrette patch di Sicurezza;
- Laddove possibile, nell'apparato è installato il sistema Antivirus aggiornato.
- Sono esclusi gli apparati che accedono ai dati personali in cloud presso terze parti o a servizi e-mail in cloud presso terze parti.

8. STRUMENTI PER LA DIDATTICA A DISTANZA

Le attività di Didattica a Distanza (DAD) sono eseguite con strumenti tra quelli selezionati come adeguati (e ove possibile indicati dal MIUR) che consentono l'accesso solo in modo riservato, autorizzato e tramite procedura di identificazione impiegando le credenziali di accesso istituzionali (identità digitale).

9. NORME COMPORTAMENTALI

9.1 Uso Corretto della -Casella di Posta

La casella di posta elettronica, assegnata dall'Istituto è uno strumento di lavoro. E' importante comprendere che un messaggio di e-mail, inviato con un indirizzo di posta dell'Istituto, è in qualche modo assimilabile ad una lettera su carta intestata; il dominio, infatti, identifica in modo univoco la fonte. L'uso della posta elettronica rispetta i seguenti principi:

- mantenere in ordine la propria casella di posta, cancellando documenti inutili e soprattutto allegati ingombranti che alla lunga potrebbero saturare lo spazio disponibile sui dischi dei computer (compreso il PC di lavoro);
- ogni comunicazione che ha contenuti rilevanti, ovvero contiene documenti da considerarsi riservati, è inviata rigorosamente ai soli Interessati;
- qualora si abbia il sospetto che un allegato ricevuto tramite posta elettronica è pericoloso, attivare il servizio STI;
- è vietato utilizzare le credenziali di un altro Incaricato per accedere, in sua assenza, alla sua posta elettronica;
- indirizzare le e-mail a destinatari secondo il criterio della "necessità di conoscere" evitando qualsiasi azione che possa essere considerata *mail spamming;*
- evitare di utilizzare la casella di posta per news letter o altre comunicazioni, non previste nelle finalità lavorative, che saturano i canali di comunicazione.

9.2 Uso Corretto di Internet

È considerato pericoloso ed è proibito (salvo diversa autorizzazione da parte del Titolare) utilizzare i computer e l'infrastruttura di rete allo scopo di:

- connettersi ai circuiti peer2peer (napster, winmx etc. etc) quando essi sono utilizzati per lo scambio abusivo di materiali protetti dal diritto di autore, per scaricare o condividere filmati, canzoni e programmi. Questo tipo di attività è in aperta violazione delle norme a tutela del diritto di autore e come tale è proibita sulla rete;
- connettersi alle reti Dark Web (TOR, I2U, FreeNet etc, etc).

Al fine di evitare la navigazione internet ai siti pericolosi o non pertinenti all'attività lavorativa, l'Istituto adotta:

- uno specifico sistema di blocco (filtro automatico) che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una 'black list';
- dove necessario, logiche di accesso a 'white lists'.

Qualora siano rilevate anomalie che potrebbero compromettere il corretto funzionamento del sistema di posta elettronica dell'Istituto, si richiede di segnalare tali anomalie al STI che provvederà alle verifiche e alle misure tutelative del caso.

9.3 Uso Corretto del Personal Computer

L'Incaricato è responsabile del PC assegnatogli o del PC su cui opera temporaneamente (in quest'ultimo caso per tutto il periodo di operatività) e deve custodirlo con diligenza. Un corretto utilizzo del PC deve prevedere:

- l'accesso al PC, alla rete (e più in generale alle informazioni conservate in formato elettronico) da parte di ciascun Incaricato è eseguito con la propria e specifica credenziale ed è proibito entrare nei PC, nella rete e nei programmi con credenziali diverse dalle proprie – salvo differenti indicazioni, in caso di emergenza, da parte del Titolare;

- Il PC non è mai lasciato incustodito. Nel caso l'Incaricato si assenta dalla sua postazione, ha l'obbligo di uscire dalla sessione di lavoro e bloccare il computer in modo che sia richiesta la password per l'accesso successivo. In alternativa è possibile impostare in automatico l'uscita ed il blocco automatico del PC dopo un prefissato tempo di inattività (es. 10 minuti) tramite, ad esempio, la funzionalità di screen saver;

- è necessario fare attenzione di non essere spiati durante la digitazione delle password ed è necessario conservare con cura le password stesse;

- tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc. ecc), contenenti dati personali o riservati di qualsiasi natura sono trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato;

- i supporti magnetici removibili possono contenere software malevolo al loro interno, evitare di installare nel proprio PC tali supporti se non riconosciuti;

- i PC sono protetti da apposito sistema antivirus. È vietato disinstallare o disattivare, anche solo temporaneamente, il programma anti virus;

- ogni Incaricato deve prestare la massima attenzione ai documenti informatici ricevuti dall'esterno, avvertendo immediatamente il STI nel caso in cui siano rilevati virus o similari. In tale caso è richiesto di disconnettere il PC dalla rete o spegnare il PC;

- non è consentito all'Incaricato effettuare modifiche all'hardware o al software del PC, salvo e previa autorizzazione da parte del STI;

- l'Incaricato è tenuto a utilizzare sul PC e sui Sistemi solo il software autorizzato dal STI ed è esplicitamente vietata l'installazione di qualsiasi software non esplicitamente autorizzato. Nel caso l'Incaricato ha bisogno di un nuovo software, ne fa richiesta al STI, che avuta l'autorizzazione a procedere dal Titolare, lo installa. I sistemi sono configurati, ove possibile, in modo che l'Incaricato non abbia i permessi per installare nuovo software.

- l’installazione e l’utilizzo di programmi finalizzati all’hackeraggio, al crackeraggio o allo spionaggio del traffico di rete è rigorosamente vietata, in caso l’Istituto rilevi che ciò è stato fatto, si riserva se ritiene, di adire ad ogni via sanzionatoria in merito;
- È consentita la navigazione su internet solo su siti legali, ben definiti.

10. MISURE ADEGUATE DI SICUREZZA

L'Istituto, nella figura del suo Titolare, riconoscendo l'importanza che la pianificazione ed implementazione di Misure di Sicurezza Informatica assume il rispetto dei principi di "privacy by design" e "by default" ed adotta le seguenti policy e misure di sicurezza informatica.

10.1 Inventario degli Asset e Classificazione dei Dati

L'Istituto appronta un inventario degli asset che contengono dati personali, indicando anche il tipo di dato contenuto in essi (personali, sensibili, sensibili medicali, biometrici, genetici, di geolocalizzazione, di traffico ed altre a seconda delle esigenze). Ad ogni asset identificato è associato un owner (persona fisica che ha la responsabilità della gestione e della concessione degli accessi all'asset stesso).

L'inventario degli asset è anche utilizzato in sede di analisi del rischio.

10.2 Sicurezza Fisica

La sicurezza dei dati richiede che l'accesso ai dati e ai documenti siano controllati. Per questo i locali che ospitano documenti e apparecchiature (uffici e locali) devono avere le corrette regole per l'accesso del personale e degli ospiti. La regola generale prevede che l'ingresso ai locali è permesso solo al personale dell'Istituto (ivi compresi gli studenti ed i genitori degli stessi), le eventuali visite di persone terze sono possibili solo se autorizzate da un responsabile di funzione.

Il controllo accessi è effettuato dal personale in portineria, presente durante l'orario lavorativo, che provvede al riconoscimento degli ospiti, alla eventuale loro registrazione e a contattare i loro riferimenti interni (es. telefonicamente) per ottenere il lasciapassare degli ospiti.

I locali che contengono dati personali (all'interno di computer o documenti cartacei) sono ad accesso controllato. Durante gli orari di lavoro devono essere costantemente presidiati dall'Incaricato e in caso di allontanamento dagli stessi, chiusi in modo da evitare che terzi possano entrare negli archivi. Si considerano eccezioni le assenze brevi (dell'ordine dei minuti) per le quali è derogato l'obbligo di cui sopra.

10.3 Telecamere

L'utilizzo delle telecamere (esterne ed interne) è consentito solamente se attivate nei periodi di assenza di presidio dal personale dell'Istituto.

Le registrazioni sono mantenute massimo 24 ore calcolate dall'inizio della registrazione.

L'accesso alle registrazioni è consentito solamente al personale autorizzato allo scopo di manutenzione tecnica oppure di visualizzazione e/o estrazione e/o cancellazione dei dati registrati.

I dati registrati possono essere visualizzati e/o estratti solamente in presenza di richiesta dell'autorità, costituisce eccezione la casistica relativa agli interventi tecnici).

10.4 Gestione dei Documenti Cartacei

Chiunque utilizzi documenti cartacei contenenti dati personali o documenti dell'Istituto riservati ha il dovere di conservarli in un luogo protetto che non sia accessibile a personale non autorizzato, quali cassetti o armadi con serratura. In alternativa è possibile lasciare i documenti sulla scrivania o in armadi aperti se è possibile chiudere a chiave l'intero ufficio per impedire accessi non autorizzati.

10.5 Software Antimalware

Su tutti i sistemi dell'Istituto è installato un apposito software antivirus e antispam. Tutti i sistemi sono configurati per ricevere automaticamente gli aggiornamenti del software antivirus e le nuove definizioni delle minacce in modo da garantire sempre il massimo dell'efficacia alla protezione. In tal modo la frequenza di aggiornamento è la più alta possibile ottenibile con il software installato e sicuramente superiore alla frequenza semestrale minima richiesta dalla legge.

Il software antivirus è configurato in modo che l'Incaricato non possa disattivare l'applicazione. Nel caso l'Incaricato abbia la percezione che il sistema possa essere stato compromesso da un virus o altro attacco informatico deve darne prontamente segnalazione all'amministratore di sistema.

10.6 Autenticazione Informatica e Autorizzazioni agli Utenti (Profilatura)

Il processo di autenticazione ha lo scopo di identificare in maniera univoca un Incaricato all'interno della struttura informatica. L'identificazione degli Incaricati che utilizzano un sistema informatico è fondamentale per la sicurezza dei dati personali, in quanto permette di attribuire con certezza le responsabilità sulle azioni effettuate sui dati personali.

Il sistema di riconoscimento dell'Incaricato è basato su credenziali di autenticazione, ovvero un codice di autenticazione (user-id) e una parola chiave (password). Ciascun Incaricato ha assegnato un codice di autenticazione personale e uno stesso codice non può, neppure in tempi diversi, essere assegnato a persone diverse. A ogni Incaricato possono essere attribuite diverse credenziali, se necessario, per svolgere ruoli diversi. E' fatto divieto all'Incaricato di comunicare le proprie credenziali ad altri.

Il sistema di autenticazione dell'Incaricato è configurato per accettare solo password di almeno otto caratteri in formato complesso (almeno un carattere alfanumerico, almeno un carattere numerico e almeno un carattere speciale) e impone all'Incaricato di modificare la password ogni tre mesi ed al primo accesso.

Le password non sono facilmente deducibili da dati personali del soggetto e non contengono termini ingiuriosi. E' attivato il sistema di history delle password che impone che le password siano diverse dalle ultime x (con x superiore a 5 configurabile) precedenti. Dopo x (con x superiore a 6) tentativi di accesso falliti (password o user-id errato) il sistema blocca automaticamente l'utenza.

Le credenziali di accesso sono autorizzate dagli owner degli asset (e dei dati in essi contenuti) e sono comunicate (user-id e password) agli Interessati usando sempre due diversi canali (es. mail e SMS oppure due differente e-mail), tramite autorizzazione esplicita all'Incaricato della creazione delle utenze (STI). Il reset della password è fatto (da STI) a seguito di tracciabile richiesta fatta esclusivamente dell'Interessato assegnatario della credenziale.

Il possesso di un codice di autenticazione di per sé non consente l'accesso ad alcun tipo di dato o di sistema. La possibilità per un Incaricato di accedere ai dati e ai sistemi dipende da un sistema di autorizzazioni (profilatura) legate alle sue credenziali di autenticazione. Ogni Incaricato ha solamente l'insieme minimo di autorizzazioni necessarie a svolgere la propria mansione. Questa regola, minimizza le autorizzazioni e quindi la possibilità di accessi non necessari ai dati.

I profili di accesso ai dati sono assegnati dagli owner degli asset dei dati.

Ricordiamo che eventuali necessità di delega per l'utilizzo di credenziali da parte di altri (da usarsi solo in casi eccezionali, quali impedimenti o prolungata assenza dell'Incaricato in cui è indispensabile e indifferibile accedere ai dati per esclusive necessità operative o di sicurezza) sono formalizzate al Titolare o ai Responsabili, che provvedono all'eventuale autorizzazione e ad informare l'ufficio personale (che tiene traccia delle deleghe formalizzate).

10.7 Sistemi di Controllo della Rete Dati

La rete interna dell'Istituto è separata dalla rete esterna (DMZ Internet) per mezzo di firewall che consentono l'accesso solo ai servizi autorizzati in modalità controllata.

I firewall sono gestiti dal STI, che provvede a gestirne gli accessi e a verificarne il corretto funzionamento. L'accesso alla rete dati dall'esterno è realizzato tramite apparati WiFi o Remote Access, che controllano gli accessi individuali, le profilazioni ed i diritti.

La rete dati dell'Istituto è gestita esclusivamente dal STI.

10.8 Salvataggio dei Dati

E' attivo un sistema di salvataggio dei dati elettronici centralizzato che esegue:

- il Full backup con cadenza giornaliera delle Banche Dati dei Documenti locali su supporto magnetico collocati all'interno dei locali sensibili;
- il Full backup con cadenza giornaliera delle Banche Dati degli Applicativi su cloud.

Il salvataggio dei dati è gestito esclusivamente dal STI.

10.9 Software, Patching e Compliance

Il software utilizzato (applicativi, database, sistemi operativi e tool di middleware e di rete) è correttamente installato alle versioni supportate e con le adeguate patch di sicurezza.

Il software utilizzato (applicativi, database, sistemi operativi e tool di middleware e di rete) è compliant con la normativa Privacy vigente.

10.10 Crittografia

Appartengono all'insieme delle 'tecniche del mascheramento dei dati' le seguenti funzionalità:

- Crittografia: processo di mascheramento (trasformazione) dei dati reversibile;
- Anonimizzazione: processo di mascheramento (trasformazione dei dati) non-reversibile;
- Pseudonominizzazione: processo di scissione dei dati reversibile.

I sistemi utilizzati (Banche Dati e Sistemi di Storage) per contenere dati stabili (data-at-rest) garantiscono comunque la possibilità di attivare almeno uno delle funzionalità di cui sopra. L'attivazione o meno di tale funzionalità è conseguenza degli esiti dell'analisi del rischio.

La trasmissione dati tra Banche Dati, Applicativi e utenti avviene in modo crittografato.

Il trasferimento massivo dei dati personali verso l'esterno (verso Banche Dati o partner esterni) avviene in forma crittografata o protetto da password.

10.11 Tracciamento Elettronico

Sono stati adottati sistemi idonei alla registrazione degli accessi e delle attività (log file) nei sistemi di elaborazione e negli archivi elettronici da parte degli Amministratori di Sistema e degli Incaricati (e-mail ed internet compresi).

Le registrazioni hanno caratteristiche di completezza, inalterabilità e integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

I tempi di conservazione dei log file sono definiti in relazione al tempo indispensabile per il perseguimento delle finalità organizzative e di sicurezza dell'Istituto. Salvo diverse indicazioni il tempo di trattenimento dei log file è 12 mesi.

Nel caso di archivi elettronici i log file contengono, per lo meno, le seguenti informazioni:

- User-Id (o equivalente che possa portare all'identificazione dell'Incaricato fisico possessore dell'user-Id);
- Data e ora dell'operazione;

- Attività svolta (login, logout, login denied, user-id creato-modificato-cancellato, opzionale altro di significativo);
- Informazioni a cui si è cercato di accedere con successo o meno;
- Livello del record di log (base, warning, debug etc etc);
- Identificativo (ip-address o nome) del server e del client utilizzati (obbligatorio solo se tecnologicamente possibile).

10.12 Cloud

Il ricorso al Cloud è consentito purchè siano rispettati i seguenti vincoli:

- I dati contenuti nel cloud sono all'interno dello spazio della Comunità Europea;
- Se i dati sono fuori dalla Comunità Europea sono eseguiti o verificati positivamente gli accertamenti previsti dalla normativa Privacy vigente: presenza di accordi tra Stati e Comunità Europea, Binding Corporate Rules (BCR) o procedimenti di Standard Contractual Clauses (SCC), altro previsto nella normativa;
- Il fornitore del servizio di Cloud garantisce la restituzione dei dati in formati leggibile se richiesto dall'Istituto;
- Il fornitore del servizio di Cloud garantisce la possibilità di crittografia dei dati personali se richiesto se richiesto dall'Istituto;
- Il fornitore del servizio di Cloud garantisce la possibilità di disporre dei log delle attività fatte dagli Incaricati se richiesto dall'Istituto;
- Il servizio Cloud è compliant con la normativa Privacy vigente.

11. ROTTAMAZIONE DI OGGETTI CONTENENTI DATI PERSONALI

Nel caso un sistema informatico (sia completo sia singole parti) è dismesso perché guasto o obsoleto, il STI verifica se contiene archivi con dati personali o dell'Istituto, ed in caso affermativo procede alla cancellazione dei dati prima di avviare il prodotto o la parte alla rottamazione o al riciclo.

Nel caso la parte contenente i dati venga rottamata è sufficiente assicurarsi che essa non sia funzionante ad esempio rompendo la sceda elettronica o forando con un trapano i piatti di un hard disk.

Nel caso la parte sia destinata al riciclo, sia all'interno dell'Istituto sia all'esterno, occorre procedere alla formattazione dell'unità di memorizzazione con un programma in grado di garantire la cancellazione sicura dei dati (es. wype program).