MINISTERO DELL'ISTRUZIONE E DEL MERITO
Istituto Tecnico Economico "Alberico Gentili"
Via Cioci, 6 - 62100 MACERATA - Tel. 0733 260500
www.itemacerata.edu.it
MCTD01000V@istruzione.it – PEC: MCTD01000V@pec.istruzione.it
C.F. 80005200433 – C.M. MCTD01000V – C.U.U. UFARVK

ALL.D ALLA DELIBERA N. 8/3 DEL CONSIGLIO DI ISTITUTO

REGOLAMENTO, POLITICHE E PROTOCOLLI PER L'UTILIZZO DELLA RETE INFORMATICA DELL'ISTITUTO SCOLASTICO A. GENTILI DI MACERATA

Approvato dal Consiglio di Istituto in data 19/12/2024

Art. 1 – Obiettivi

Il presente Regolamento ha i seguenti obiettivi:

- **prevenire**, ove possibile, comportamenti anche inconsapevoli che possano minacciare o compromettere la sicurezza nel trattamento dei dati, il rispetto della normativa sul diritto d'autore, e/o l'accesso stesso alle risorse di Istituto;
- **codificare** le regole di comportamento da seguire per un corretto utilizzo degli strumenti e servizi onde evitare problemi, disservizi, costi aggiuntivi e rischi per la sicurezza dei dati e del patrimonio dell'Istituto;
- **preservare** la sicurezza nell'accesso alla rete interna e alla rete Internet;
- **garantire** il rispetto delle leggi in materia di utilizzo delle risorse informatiche per l'elaborazione dei dati personali ai sensi del GDPR, Provvedimenti del Garante della Privacy collegati e normativa nazionale di settore;
- **informare** con chiarezza gli interessati sulle attività di monitoraggio e controllo;
- **diffondere** una cultura della sicurezza che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.
- **Codificare** i protocolli di lavoro per la gestione delle identità digitali per la fruizione dei servizi informatici erogati;
- **Individuare** il settori ed il personale coinvolto nella gestione delle reti di Istituto e nella gestione delle identità digitali

Art. 2 - Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso, di uso della rete informatica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire all'interno e all'esternodell'Istituzione scolastica.

La rete dell'Istituzione scolastica è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.

Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica della scuola. Il patrimonio informatico è l'insieme delle banche dati in formato digitale ed

in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

In particolare la rete di Istituto è strutturata in due nodi principali: la RETE didattica con dominio gentili.local e la RETE di segreteria con dominio itcgentili.local

Il presente regolamento si applica a tutti gli utenti interni ed esterni che sono autorizzati ad accedere alla rete della scuola. Per utenti interni si intendono tutti gli amministrativi, i docentie i collaboratori scolastici, nonché gli studenti. Per utenti esterni si intendono le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse, i collaboratori esterni e tutti gli altri soggetti non appartenenti all'Istituto autorizzati all'accesso alla rete di Istituto e alla fruizione dei servizi ad essa collegati.

Art. 3 – Principi generali – Diritti e Responsabilità

L'Istituzione scolastica promuove l'utilizzo della rete informatica, di internet e della posta elettronica, quali strumenti utili a perseguire le proprie finalità istituzionali.

Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati.

Il presente regolamento considera i divieti posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113,114, e 184, comma 3, del Codice; artt. 4 e 8 legge 20 maggio 1970, n. 300), rispettando durante i trattamenti i principi di necessità (art. 3 del Codice; par. 5.2), correttezza (art. 11,comma 1, lett. a) e finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b del Codice par. 4 e 5).

Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete informatica è sottoposta a registrazione dei log al fine di ricondurre le attività di una determinata risorsa di rete ad una identità digitale.
Detti log possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo al fine della tutela del patrimonio scolastico (ad esempio in caso di danni ad un'infrastruttura di rete verificare l'utilizzatore della stessa), e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente o dell'autorità di controllo in caso di violazione della normativa sulla privacy e databreach. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D. Lgs. n. 196/2003 e ss.mm.ii..

Art. 4 – Controlli e monitoraggio

L'identificazione dei passi da adottare per definire i livelli di rischio informatico è estratta dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC "CIS Critical Security Controls for Effective Cyber Defense" nella versione 6.0 del 2015, e trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, in un equilibrato bilanciamento trai costi di vario genere che l'implementazione di una misura di sicurezza richiede e i benefici che la stessa è in grado di offrire. L'elenco dei 20 controlli in cui esso si articola, normalmente riferiti comeCritical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi. In particolare, ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla propria.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI A DISPOSIZIONE DEI DIPENDENTI E DEGLI STUDENTI. L'Istituto si impegna a provvedere alla redazione di un inventario dei dispositivi messi a disposizione di dipendenti e studenti. In attesa della redazione completa di un inventario di tutti i dispositivi autorizzati i controlli vengono assicurati dai protocolli di gestione delle identità digitali (allegato 1) e dalla relativa politica riconducibilità di ogni azione condotta su una risorsa di rete ad un determinato soggetto.
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUIDISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE
ABSC 10 (CSC 10): COPIE DI SICUREZZA
ABSC 13 (CSC 13): PROTEZIONE DEI DATI
L'Istituto regola il traffico consentito in ingresso e in uscita dalla rete e mediante tecnologie di filtro dei contenuti (vedi allegato ***Politica di filtro sul traffico di rete***) può preventivamente limitare o impedire l'accesso a servizi e/o contenuti che ritiene a suo insindacabile giudizio:

- illeciti;
- non appropriati;
- pericolosi per la sicurezza dei dati e delle persone;
- non pertinenti lo svolgimento dell'attività lavorativa.

Qualora risultassero non accessibili anche risorse che l'utente ritiene necessarie, egli può produrre una richiesta debitamente motivata all'Amministratore di Sistema competente al fine di revocare il blocco in via temporanea o definitiva.

L'Istituto si riserva il diritto di controllare l'accesso, l'utilizzo e il funzionamento dei servizi informatici da esso erogati, sia tramite sistemi di monitoraggio automatico centralizzato, sia tramite agenti installati sulle postazioni, sia durante gli interventi di manutenzione; si riserva inoltre il diritto di mantenere registri delle attività (log) di vario tipo inerenti i servizi nel rispetto della normativa vigente di trattamento dei dati personali (vedi allegato ***Politica di gestione dei log***, che dettaglia le fonti da cui si raccolgono i log e le modalità di gestione)

Tali controlli sono finalizzati esclusivamente a:

- ottemperare alla normativa cogente in materia protezione dei dati e del diritto d'autore ed in particolare alle richieste dell'autorità di controllo in materia;
- rispondere ad eventuali richieste dell'autorità giudiziaria;
- garantire la sicurezza dei servizi anche tramite sistemi per la verifica delle intrusioni informatiche (IDS);
- verificare la corretta gestione dei flussi di dati e informazioni;
- implementare l'inventario delle risorse in rete e dei software utilizzati;
- svolgere attività relative a modifiche tecniche/operative;
- verificare la corretta configurazione dei sistemi;
- raccogliere e preservare le evidenze forensi a supporto di ogni eventuale azione legale che coinvolga l'Istituto;
- contrastare utilizzi impropri e/o illeciti e più in generale contrari alla politica di uso accettabile delle risorse tecnologiche di Istituto;
- monitorare l'uso delle credenziali esposte.

È escluso ogni utilizzo dei dati raccolti per fini diversi da quelli sopra citati, in particolare per qualunque forma di controllo a distanza degli utenti al fine del controllo delle performance o dell'irrogazione di sanzioni disciplinare, al di fuori dei casi in cui le stesse siano conseguenza del compimento di reati per i quali le stesse siano previste.
L'accesso ai registri delle attività (log) è consentito solo al personale autorizzato e riguarda in primo luogo dati aggregati non riferibili a un singolo utente. L'accesso ai dati di utilizzo di un singolo utente, laddove necessario, avviene per giustificati motivi. In nessun caso sono ammessi controlli prolungati e costanti.
Alcune attività (ad es. amministratori di sistema) sono raccolte e gestite in adempimento alla normativa vigente.

Art. 5 – Gestione degli incidenti di sicurezza

Gli incidenti vengono tracciati su apposito registro secondo modalità previste nell'allegato ***Politica di gestione degli incidenti di sicurezza.***
Tutti gli utenti hanno l'obbligo di segnalare tempestivamente ogni anomalia nel funzionamento del sistema informativo di Istituto o qualsiasi comportamento volontario o accidentale, anche di terzi esterni all'Istituto, che possa esporre i dati oggetto del trattamento al rischio di furto, perdita o modifica non autorizzata. Nel caso si sospetti una compromissione degli strumenti informatici da parte di un malware o di un soggetto esterno all'Istituto, questa deve essere segnalata prima possibile agli amministratori di sistema o ai responsabili di servizio o di settore.
Le misure di sicurezza preventive adottate dall'Istituto e i comportamenti responsabili messi in atto dai collaboratori riducono la probabilità che si verifichi un incidente di sicurezza, ma non la annullano, pertanto è molto importante che ogni situazione anomala venga gestita nel modo corretto, anche per mettere in condizione l'Istituto di rispondere tempestivamente a tutti gli obblighi di legge in materia di protezione dei dati.
Un incidente di sicurezza non deve mai essere nascosto, ed è obbligatorio che in caso di sospetta compromissione di uno strumento di lavoro o delle credenziali di accesso personali, l'utente coinvolto si attenga a questo semplice protocollo:

- non spegnere per nessuna ragione il dispositivo (ad es.: PC, Smartphone, etc.);
- interrompere il collegamento alla rete dati (ad es. staccare il cavo di rete, disabilitare il WIFI. etc.);
- non cancellare niente dal dispositivo perché i dati raccolti possono essere fondamentali per l'analisi e la risoluzione dell'incidente;
- segnalare immediatamente l'anomalia come potenziale incidente di sicurezza e attenersi alle istruzioni che verranno impartite.

Art. 6 – Limitazione dell'utilizzo di risorse

A seguito della rilevazione di un incidente informatico e/o per rispondere a richieste delle Autorità Investigative e in considerazione della possibilità di dover rispondere ad eventuali obblighi legali di rispetto della catena di custodia volta a preservare evidenza di incidenti particolarmente gravi, l'Istituto può:

- limitare o impedire l'uso del dispositivo (ad es.: esclusione dalla rete di Istituto) o l'accesso ai servizi di Istituto;
- chiedere la consegna del dispositivo per il tempo necessario a compiere le attività di analisi e risoluzione

dell'incidente;

- imporre il ripristino sicuro e verificato dai tecnici ASI del dispositivo come condizione necessaria per l'accesso ai servizi di Istituto.
- inibire l'accesso alla rete da parte dell'utente per il tempo necessario a compiere le attività di analisi e risoluzione dell'incidente.

Art. 7 – Settori e risorse umane preposte alla gestione delle reti e al rispetto del presente regolamento

Le operazioni e i controlli previsti dal presente regolamento possono essere poste in essere solamente dai soggetti individuati nello stesso o espressamente incaricati dal Dirigente Scolastico.
In particolare il referente Tecnico di Istituto, gli Amministratori di Sistema, e l'assistente amministrativo addetto alla gestione degli account di sistema, nominati dal Dirigente Scolastico con provvedimento esplicito provvedono a:

- inserire a dominio nuove risorse registrando il collegamento tra la risorsa e il nome di dominio;
- configurare le workstation e i notebook;
- gestire il sistema delle identità digitali provvedendo alla creazione e cancellazione delle stesse;
- conservare e registrare i log di accesso e provvedere ad un monitoraggio periodico e generico degli stessi segnalando i casi di attività sospette al Dirigente Scolastico;
- provvedere all'aggiornamento e alla manutenzione delle risorse di rete;
- promuovere il miglioramento della gestione delle reti e dei servizi informatici dell'Istituto;
- provvedere alla catalogazione e all'istallazione dei software autorizzati;

Dette operazioni debbono essere poste in essere esclusivamente da personale in possesso di credenziali di amministratore di sistema.

a) Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno.

b) Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica istituzionale, secondo le direttive dal Titolare, in particolare aggiornare e controllare **quotidianamente il foglio di lavoro delle identità digitali.**

c) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

d) conservare e registrare i log di accesso e provvedere ad un monitoraggio periodico e generico degli stessi.

e) Compiere periodicamente un analisi della vulnerabilità delle risorse informatiche di Istituto.

f) Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, attesa l'autorizzazione del Titolare, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

g) Provvedere all'inventario dei software autorizzati.

h) Provvedere all'inventario delle risorse informatiche di proprietà dell'Istituto messe a disposizione dei dipendenti e degli studenti dell'Istituto

i) Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

j) Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Dette operazioni debbono essere poste in essere esclusivamente da personale in possesso di credenziali di amministratore di sistema, ad esclusione di quelle di cui b), che possono essere poste in essere dall'assistente amministrativo addetto alla gestione degli account di sistema, secondo le proprie competenze.

I settori preposti alle reti di Istituto sono:
UFFICIO DEI SERVIZI INFORMATICI DI ISTITUTO: ne fanno parte di diritto il Dirigente Scolastico e il Direttore dei Servizi generali e Amministrativi, oltre al Responsabile Tecnico di Istituto, ha compiti di coordinamento di tutto il personale addetto alla gestione delle reti di Istituto e dei servizi informatici, con particolare riferimento agli amministratori di Sistema incaricati, con provvedimento formale, della gestione e/o della manutenzione di uno o più sistemi collegato/i alle Reti di Istituto.
SETTORE AMMINISTRAZIONE DI RETE INFORMATICA DIDATTICA, preposto a garantire il rispetto del presente regolamento per la rete locale gentili.local
Il settore si avvale di
Un Referente Tecnico di Istituto
Quattro Amministratori di sistema interni
Due Amministratori di sistema esterni che garantiscono interventi di manutenzione su richiesta degli amministratori interni
SETTORE AMMINISTRAZIONE DI RETE AMMINISTRATIVA, preposto al rispetto preposto a garantire il rispetto del presente regolamento per la rete locale ITCGENTILI.local
Il settore si avvale di
Due amministratore di sistema interno
Uno/due Amministratori di sistema esterni che garantiscono interventi di manutenzione su richiesta degli amministratori interni
Con riferimento al Provvedimento del 27 Novembre 2008 del Garante della Privacy, sono da considerare, a tutti gli effetti, Amministratori di Sistema i soggetti che, in viacontinuativa, svolgono operazioni di:

1) Amministrazione di Sistemi Informatici (System Administrator)
2) Amministrazione di Server (Server Administrator)
3) Amministrazione di Sistemi di Rete (Network Administrator)
4) Amministrazione di Sistemi di Sicurezza (Security Administrator)
5) Amministrazione di Software e Applicazioni (Application Administrator)
6) Amministrazione di Database (Database Administrator)
7) Amministrazione di Sistemi di Salvataggio Dati (Backup / Storage Administrator)
8) Amministrazione di Sistemi di Ripristino Dati (Recovery Administrator)
9) Amministrazione di Siti Web (Web Administrator)
10) Altri soggetti addetti alla gestione o alla manutenzione di strumenti elettronici che, per l'espletamento delle loro funzioni, devono compiere operazioni di amministrazione
11) Amministrazione di Apparati Hardware (Hardware Administrator).

Art. 8 – Utilizzo del personal computer

Il personal computer affidato al dipendente e agli studenti è uno strumento di lavoro e didattico. Ogni utilizzo non inerente all'attività istituzionale può contribuire ad innescare disservizi, costi di manutenzioni e, soprattutto, minacce alla sicurezza e pertanto è vietato.

In particolare:

a) La configurazione della workstation è a carico dell'AdS di riferimento, che ne registra il nodo in rete, rilascia le credenziali agli utenti e cura la registrazione e conservazione dei log di accesso (vedasi politica di conservazione dei log)

b) L'accesso all'elaboratore deve essere protetto da password. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'amministratore di sistema incaricato.

c) L'amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, avrà la facoltà di accedere in qualunque momento anche da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al personal computer di ciascuno.

d) Il personal computer deve essere spento ogni sera, **o al termine delle lezioni**, prima di lasciare gli uffici o i laboratori di informatica, o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i personal computer lo screensaver e la relativa password.

e) L'accesso ai dati presenti del personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

f) E' vietato installare autonomamente programmi informatici **sui server/client** salvo autorizzazione esplicita dell'amministratore di sistema, in quanto sussiste il grave pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre lastruttura a gravi responsabilità civili e anche penali in caso di violazione della normativaa tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

g) E' vietato modificare le caratteristiche impostate sul proprio Pc, salvo con autorizzazione esplicita dell'amministratore di sistema.

h) E' vietato inserire password locali alle risorse informatiche assegnate (come ad esempioche non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate all'amministratore di sistema.

i) E' vietata l'installazione sul proprio Pc di dispositivi di memorizzazione, comunicazione oaltro (come ad esempio masterizzatori, modem, pendrive, dischi esterni, i-pod, telefoni ecc..), se non con l'autorizzazione dell'amministratore di sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore di sistema di riferimento nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

j) Per le postazioni multiutente come notebook dei laboratori e delle classi è necessario effettuare l logout alla fine di ogni ora o comunque quando l'utente lascia la postazione rimettendola nella disponibilità di altri utenti.

Art. 9 – Utilizzo della rete informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.

Si parte quindi dal presupposto che i file relativi alla produttività individuale vengono salvati sulserver e i limiti di accesso sono regolarizzati da apposite procedure di sicurezza che suddividono gli accessi tra gruppi e utenti.

L'amministratore di sistema incaricato può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza o in violazione del presente regolamento sia sul Pc degli incaricati sia sulle unità di rete.

Le password di ingresso alla rete ed ai programmi sono segrete e non vanno comunicati a terzi.

Costituisce buona regola la periodica (almeno ogni 6 mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Pc se non strettamente necessarie (e per breve tempo) allo scambio dei file con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di minare la sicurezza dell'intero sistema.

E' compito dell'amministratore di sistema incaricato provvedere alla creazione e alla manutenzione di aree condivise sul server per lo scambio dei dati tra i vari utenti.

Nell'utilizzo della rete informatica è fatto divieto di :

a) Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento.

b) Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.

c) Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc…).

d) Installare componenti hardware non compatibili con l'attività istituzionale.

e) Rimuovere, danneggiare o asportare componenti hardware.

f) Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attivitàdi altri utenti, per leggere, copiare o cancellare file e software di altri utenti.

g) Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazionedi tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy.

h) Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

I servizi di rete possono essere fruiti da tutti gli utenti profilati dal sistema di identity management.
L'accesso ai servizi di rete per utenti esterni avviene sotto controllo di un AdS tramite fornitura di identità digitali provvisorie registrando l'autorizzazione all'utilizzo.
L'accesso ad ogni servizio dovrà essere sospeso in automatico alla data di fine del periodo temporale di autorizzazione.

Art. 10 – Utilizzo di internet

I Pc abilitati alla navigazione in Internet costituiscono uno strumento necessario allo svolgimento dell'attività lavorativa e didattica.

Nell'uso di internet e della posta elettronica NON sono consentite le seguenti attività:

a) L'uso di internet per motivi personali.

b) L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc..).

c) Lo scaricamento (download) di software e di file non necessari all'attività istituzionale e non autorizzati da competete Amministratore di Sistema.

d) Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer.

e) Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali.

f) Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

Art. 11 – Utilizzo della posta elettronica

La casella di posta, assegnata dall'Istituto, è uno strumento di lavoro e didattico e le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.

E' fatto divieto di utilizzare le caselle di posta elettronica della struttura per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione, che esulino dagli scopi della scuola.

E’ buona norma evitare messaggi contemporaneamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellandodocumenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegnicontrattuali o precontrattuali con l’Istituto ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Direttore dei Servizi Generali Amministrativi, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all’esterno senza previa autorizzazione del Responsabile del trattamento.

Per la trasmissione di file all’interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

E’ obbligatorio controllare i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non riconosciuti) e accertarsi dell’identità del mittente.

In particolare nell’uso della posta elettronica *NON* sono consentite le seguenti attività:

a) La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D. Lgs. 196 del 30/06/2003) e inerenti le ragioni di servizio.
b) L’apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell’identità del mittente.
c) Inviare tramite posta elettronica user-id, password, configurazioni della rete interna,indirizzi e nomi dei sistemi informatici.

Art. 12 – Utilizzo della wi fi

Il servizio è fruibile esclusivamente per il personale attraverso le proprie credenziali di Istituto.
Il servizio di rete WI-FI è fornito mediante l'utilizzo di frequenze in banda condivisa, la fruizione quindi del servizio e la sua qualità non sono garantite.
L’Istituto non è responsabile verso l'utente e/o verso terzi per i danni diretti o indiretti, derivanti da sospensioni o interruzioni del servizio.
L’utilizzo è comunque soggetto al rispetto delle norme vigenti, delle condizioni contenute nel presente regolamento e delle regole tecniche, che si intendono implicitamente accettate con il primoutilizzo del servizio stesso.
Il servizio WI-FI viene autorizzato/de autorizzato per singolo utente e per ruolo; non si prevede redemption time, nè periodo di pending delete. La disattivazione avverrà alla scadenza del periododi autorizzazione e/o del ruolo.
La registrazione di utenti ospiti e la creazione di un account temporaneo per convegni, meeting e manifestazioni e eventi simili sono a cura degli AdS locali e/o del Settore preposto e dovrà avvenire manualmente o attraverso un sistema automatico, con garanzia dell’individuazione dell’utente.
Ai fini della sicurezza dell’intera rete di Istituto, è vietato istallare apparati Access Point non autorizzati e

connetterli alla rete wired, e/o creare sotto reti.

Art. 13 – Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoletidevono essere consegnati all'Amministratore di Sistema D.S.G.A. per l'opportuna distruzione.

Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema addetto provvederà alla formattazione ovvero alla distruzione delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Art. 14 – Utilizzo di PC portatili / Tablet

L'utente è responsabile del PC portatile/Tablet assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili/Tablet si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili/Tablet utilizzati all'esterno (convegni, lavoro domestico autorizzato, ecc…) in caso di allontanamento devono essere custoditi in un luogo protetto.

Art. 15 – Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di naturastrettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessarie e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documentio file non adatti (molto lunghi o non supportati, come ad esempio il formato PDF o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Art. 16 – Utilizzo delle risorse cloud

Tutti i servizi web devono essere implementati nel rispetto dei principi di sicurezza del dato, in aderenza al modello privacy-by-default e privacy-by-design. La divulgazione e/o pubblicazione dei dati deve avvenire nel rispetto delle norme sulla privacy.
In particolare, l'interfaccia web deve comunicare attraverso protocollo SSL, non deve permettere

crosscript ed escalation protocol, deve essere implementata, possibilmente, su un server in zonaDMZ, oppure attraverso l'opportuna configurazione di VLAN o di zone di servizi gestiti da firewall. L'applicativo web deve comunicare in modo esclusivo con la relativa base dati su protocollo protetto
o controllato e non deve permettere la consultazione o l'accesso diretto al dato.
In accordo con le misure minime di sicurezza, tutti i servizi web devono essere registrati su registro informatico. In questo devono essere registrate tutte le informazioni delle specifiche tecniche e delle relative dipendenze funzionali da altri servizi.
Per le profilazioni degli utenti si deve far riferimento all'allegato protocollo di gestione del sistema delle identità digitali di Istituto

Art. 17 – Osservanza delle disposizioni in materia di Privacy

E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D. Lgs. n. 196/2003 e ss.mm.ii..

Art. 18 – Non osservanza del regolamento

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari (modifica regolamento disciplina istituto) nonché con le azioni civili e penali consentite.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla rete informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigente.

Art. 19 – Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.

Allegato 1 Protocollo di gestione delle identità digitali e policy delle password

Identità digitali del personale:

Il personale in servizio presso l'Istituto all'atto dell'assunzione deve essere profilato per i seguenti servizi:

- Fruizione della Rete di Segreteria di Istituto per il Personale Amministrativo e Tecnico e per i collaboratori del Dirigente.
- Fruizione delle risorse cloud dell'Istituto per il Personale Amministrativo, Tecnico e Ausiliario e per il personale docente
- Fruizione dell'e-mail Istituzionale
- Fruizione delle risorse cloud dell'Istituto per gli studenti
- Fruizione della rete didattica per i docenti
- Fruizione della rete didattica per gli studenti

Gestione della Profilazione del personale dipendente a tempo determinato e indeterminato

1) **All'atto dell'assunzione gli assistenti amministrativi addetti al personale faranno compilare e sottoscrivere l'allegato modulo al dipendente neoassunto, nel quale dovrà essere esplicitata anche il consenso al possibile monitoraggio dell'attività in rete associata alla propria identità digitale e l'accettazione del presente regolamento.**

2) **Successivamente il neoassunto verrà inserito nell'allegato foglio di lavoro condiviso per la gestione delle identità digitali a disposizione degli Amministratori di Sistema, dell'incaricato di segreteria di gestione degli account Spaggiari, del Dirigente Scolastico, del DSGA e dei responsabili di settore ai fini del controllo**

3) **Quindi per i neoassunti che prendono servizio al primo settembre di ogni anno, entro i due giorni successivi all'assunzione, o comunque in tempo utile per l'inizio delle lezioni di ogni anno scolastico:**

- **Gli amministratori di sistema addetti al settore provvederanno alla creazione di un account di rete per -l'accesso alla rete di segreteria/didattica a seconda del ruolo di inquadramento specificando che l'accesso alla rete didattica è riservato al personale docente e ai collaboratori scolastici addetti e agli assistenti tecnici mentre l'accesso alla rete di segreteria è riservato al Dirigente Scolastico, ai collaboratori del Dirigente Scolastico, al personale di segreteria, alle funzioni strumentali e al DSGA, COLLEGANDO ALLO STESSO I PRIVILEGI CONNESSI AL RUOLO DI INQUADRAMENTO;**
- **Gli amministratori di sistema addetti al settore provvederanno alla COMUNICAZIONE DELL'ACCOUNT MICROSOFT OFFICE AL DIPENDENTE**
- **L'assistente amministrativo addetto alla gestione degli account ovvero i responsabili di settore provvedono alla creazione di un account per la gestione della google suite.**
- **L'assistente amministrativo addetto alla gestione degli account provvede alla creazione dello stesso in relazione all'inquadramento del dipendente riportato nel foglio di lavoro condiviso;**

- **Di tutte le suddette operazioni deve essere dato conto nel foglio condiviso di gestione delle identità digitali.**

4) **Per i neoassunti che prendono servizio successivamente all'inizio dell'anno scolastico:**

- **Per gli ATA l'assistente amministrativo addetto alla gestione degli account provvede alla creazione dello stesso in relazione all'inquadramento del dipendente riportato nel foglio di lavoro condiviso**

- **Gli amministratori di sistema addetti al settore segreteria provvederanno alla creazione di un account per l'accesso alla rete di segreteria entro due giorni dalla presa di servizio in relazione all'inquadramento del dipendente riportato nel foglio di lavoro condiviso**

- **Per i docenti l'assistente amministrativo addetto alla gestione degli account provvede, alla presa di servizio, alla consegna in busta chiusa di un account per l'accesso alla rete didattica valevole per 15 giorni;**

- **Per i docenti e i collaboratori scolastici gli amministratori di sistema addetti al settore didattica provvederanno, in relazione all'inquadramento del dipendente riportato nel foglio di lavoro condiviso, alla creazione di un account per l'accesso alla rete didattica entro quindici giorni, all'invio dello stesso e all'eventuale reset dell'identità provvisoria;**

- **Gli amministratori di sistema addetti al settore provvederanno alla COMUNICAZIONE DELL'ACCOUNT MICROSOFT OFFICE AL DIPENDENTE**

- **L'assistente amministrativo addetto alla gestione degli account ovvero i responsabili di settore provvedono alla creazione di un account per la gestione della google suite.**

- **Di tutte le suddette operazioni deve essere dato conto nel foglio condiviso di gestione delle identità**

5) **Per gli studenti neoiscritti:**

- **L'assistente amministrativo addetto alla gestione degli account provvede alla creazione dello stesso;**

- **L'assistente amministrativo addetto alla gestione degli account ovvero i responsabili di settore provvedono alla creazione di un account per la gestione della google suite;**

- **Gli amministratori di sistema addetti al settore provvederanno alla creazione di un account per l'accesso alla rete didattica entro l'inizio dell'anno e all'invio dello stesso**

- **Gli amministratori di sistema addetti al settore provvederanno alla COMUNICAZIONE DELL'ACCOUNT MICROSOFT OFFICE ALLO STUDENTE**

Gestione della Profilazione di soggetti esterni all'amministrazione autorizzati all'accesso ai servizi informatici di Istituto:

- **L'assistente amministrativo addetto agli account registra le istanze di accesso ai servizi informatici di Istituto, autorizzate dal Dirigente Scolastico, nel foglio di lavoro condiviso "richieste accesso ai SI" allegato al presente, indicando nello stesso il numero si identità digitali richieste;**

- **Gli amministratori di sistema addetti al settore provvederanno, tempestivamente e comunque entro 4 giorni dall'autorizzazione, alla creazione dei richiesti account di rete per l'accesso alla rete didattica**

PENDING DELETE TIME

Di seguito vengono riportate le tempistiche secondo cui l'assistente amministrativo addetto alla gestione degli account e gli amministratori di sistema provvedono alla cancellazione degli account di accesso ai diversi servizi:

- **SERVIZI SPAGGIARI: 30 GIORNI DALLA CESSAZIONE DEL RAPPORTO**
- **SERVIZIO DI POSTA ELETTRONICA DI ISTITUTO: 60 GIORNI DALLA CESSAZIONE DEL RAPPORTO**
- **ACCESSO ALLA RETE INFORMATICA DI ISTITUTO: 15 GIORNI DALLA CESSAZIONE DEL RAPPORTO**
- **SERVIZIO FRUIZIONE SUITE OFFICE: 30 GIORNI DALLA CESSAZIONE DEL RAPPORTO**

Per gli utenti esterni all'amministrazione l'account deve essere resettato immediatamente al termine del periodo di autorizzazione.

POLITICA DELLE PASSWORD DEI SERVIZI INFORMATICI DI ISTITUTO

Questa politica si applica sia agli utenti che devono utilizzare le credenziali loro assegnate per accedere a strumenti e servizi che trattano i dati dell'Istituto, sia a chi deve realizzare e gestire dei sistemi di autenticazione

Regole di composizione e gestione delle password

Tipo di regola	Contenuto regola
Obbligatoria	La password deve contenere almeno 8 caratteri. La password deve contenere i seguenti tipi di caratteri: • Lettere minuscole da a alla z; • Lettere maiuscole dalla A alla Z; • Numeri da 0 a 9; • Caratteri speciali (es. !, $, #, ^, %,*,ecc.). La password deve contenere almeno un numero, una lettera maiuscola e un caratterespeciale. La password deve essere modificata entro 90 giorni. La password deve essere diversa dalle password utilizzate nell'ultimo anno. La password non deve essere riconducibile all'identità del titolare dell'account.
Obbligatoria	Le password non devono essere condivise con nessuno, nemmeno con assistant iamministrativi, segretari, colleghi e familiari.
Obbligatoria	Le password non devono essere inserite nei messaggi di posta elettronica o in altreforme di comunicazione elettronica insieme al nome dell'utente o a qualsiasi altra informazione relativa al servizio (es. sito di accesso al servizio).
Obbligatoria	Le password non devono essere annotate e memorizzate in nessun posto all'interno del luogo di lavoro.
Obbligatoria	Le password non devono essere memorizzate in un file su un sistema informatico o sudispositivi mobili (es. telefono, tablet) senza crittografia.
Obbligatoria	La funzione «Ricorda la password» delle applicazioni (es. browser web) non deve essere utilizzata se non con programmi di gestione avanzati che utilizzano sistemi dicrittografia forte.
Obbligatoria	Gli account con privilegi da amministratore devono avere una password diversa dagliaccount standard e devono prevedere almeno l'autenticazione a due fattori.
Consigliata	Si raccomanda di **non utilizzare la stessa password** dell'utenza federata di Istituto(IDEM) **per altri account** non federati o esterni.

Consigliata	Si raccomanda di non utilizzare password contenenti **informazioni personali**, in quanto sono facili da indovinare o scoprire (ad es. numero di telefono dell'utente,nome, compleanno dei figli, anniversari etc.)
Consigliata	Si raccomanda di non utilizzare parole di uso comune, o contenute in un dizionario,perché possono essere facilmente indovinate.
Consigliata	Se si sospetta che una password non sia più sicura o affidabile, deve essere cambiata immediatamente
Consigliata	Le password devono essere bloccate dopo 5 tentativi sbagliati nell'arco di tempo di 10minuti. Dopo 40 false inserzioni nell'arco di 24 ore, le credenziali possono essere sbloccate solo contattandogli ads.

Allegato 2 – Politica di gestione degli incidenti informatici

1. Scopo del documento

Lo scopo di questo documento è definire la corretta gestione degli incidenti di sicurezza IT. Una buona gestione degli incidenti informatici è utile a proteggere i dati personali di cui l'Istituto è titolare, garantire la sicurezza delle informazioni e dei sistemi impiegati per il loro trattamento, oltre che minimizzare l'impattosui servizi erogati e sull'operatività degli utenti. In particolare il documento indica le linee guida affinché gli incidenti di sicurezza informatica:

- vengano rilevati e analizzati tempestivamente;
- vengano gestiti adeguatamente;
- abbiano un impatto ridotto al minimo;
- vengano intraprese le azioni di contenimento necessarie per prevenire ulteriori danni;
- gli incidenti e le corrispettive azioni di mitigazione vengano registrate e documentate;
- le autorità competenti o gli interessati siano informati tempestivamente come richiesto dallenormative vigenti.

2. Ambito di applicazione

La politica descritta in questo documento si applica al perimetro informatico dell'Istituto. Questo perimetro ha dei contorni mutevoli che nel corso del tempo tendono ad assumere caratteristiche e dimensioni sempre meno circoscritte. Il perimetro informatico dell'Istituto è costituito da: sistemi informatici, servizi, processi e procedure che utilizzano software e hardware, ma anche da utenti con prassi e consuetudini diverse. Tutte le componenti di questo perimetro informatico, da quelle più fisiche a quelle immateriali, possono subire o generare un incidente informatico, o comunque esserne coinvolte almeno in parte.

3. Cosa sono gli incidenti di sicurezza informatica

Un incidente di sicurezza informatica è un evento che tende o può compromette i principi di integrità, riservatezza e disponibilità di informazioni gestite dall'Istituto tramite strumenti informatici. Un evento che non abbia queste caratteristiche, benché possa creare disagio agli utenti o danno economico all'Istituto, non deve essere considerato un incidente di sicurezza informatica. Viene classificato come incidente di sicurezza informatica anche un evento che non consenta di adempiere gli obblighi di legge o espone l'organizzazione al rischio di incorrere in sanzioni o dover procedere a risarcimenti per eventuali danni cagionati. Di seguito un elenco non esaustivo di eventi che costituiscono un incidente di sicurezza informatica:

- accesso non autorizzato a banche dati, sistemi informatici, reti o relativi apparati;
- accesso non autorizzato al perimetro dell'Istituto dove si trovano strumentazioni o apparatiinformatici ad accesso limitato;
- diffusione o divulgazione non autorizzata di informazioni;
- compromissione dell'integrità dei sistemi o delle informazioni;
- impossibilità di accesso ad informazioni trattate dall'Istituto;
- malfunzionamento di qualsiasi natura dei sistemi di controllo, accesso e sorveglianza;
- danneggiamento fisico o logico delle risorse contenenti informazioni, o necessarie alla loro elaborazione, con conseguente perdita o riduzione di integrità, riservatezza e disponibilità delle informazioni;
- diffusione di malware all'interno dell'infrastruttura informatica, etc.

4. Cosa sono le violazioni di dati personali (Data Breach)

La violazione dei dati personali trattati dall'Istituto, detto anche "Data Breach", è un particolare tipo di incidente di sicurezza informatica che determina - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati dall'Istituto (come definito nel Regolamento UE 679/2016 - GDPR). Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Dato personale è qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Si considera identificabile la persona fisica che può essere riconosciuta, direttamente o indirettamente, attraverso dei dati che lo caratterizzano, per esempio nome e cognome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (GDPR, art. 4). Le violazioni di dati personali possono verificarsi in un ampio numero di casi, a titolo di esempio riportiamo:

- smarrimento o furto di attrezzature informatiche che contengono datipersonali (es.: pc portatili, chiavette etc.);
- invio di messaggi contenenti dati personali a un destinatario sbagliato;
- pubblicazione di dati personali su risorse informatiche accessibili al pubblico (es.: pubblicazione su siti web dell'Istituto di dati personali).
- divulgazione di dati confidenziali a persone non autorizzate;
- accesso abusivo (es.: data breach causato da un accesso non autorizzato ai sistemi);
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo proprietario;
- violazione di misure di sicurezza fisica (ad esempio, forzatura di porte o finestre di stanze di sicurezzao archivi, contenenti informazioni riservate);

5. Classificazione degli incidenti di sicurezza informatica

Una classificazione degli incidenti di sicurezza informatica, insieme a un'adeguata analisi e documentazione delle informazioni relative all'incidente, è di fondamentale importanza per una risposta tempestiva ed efficace. A seconda dell'impatto che un incidente ha sull'organizzazione e sulle capacità degli utenti di adempiere alle loro mansioni viene adottata la seguente valutazione.

Impatto	Descrizione
Basso	- Non causa danni significativi a operatività, produttività, amministrazione e gestione - Causa una perdita di fiducia trascurabile - Coinvolge solo dati non classificati - L'Impatto sulla integrità delle informazioni è trascurabile o secondario con scarso effetto sull'attività - Comporta una perdita di disponibilità delle informazioni che può essere tollerata fino a due/tre giorni - Causa perdite economiche e danni trascurabili
Medio	- Potrebbe causare interruzioni di attività interne all'organizzazione - Potrebbe degradare l'effettiva operatività in una parte dell'organizzazione - Può causare una limitata pubblicità negativa - Comporta una perdita di disponibilità delle informazioni che può essere tollerata fino a un giorno - Potrebbe causare una violazione minore o tecnica di obblighi legali o normativi

Alto	- Può causare interruzioni delle attività proprie dell'organizzazione con qualche ripercussione anche in altre organizzazioni - Può compromettere l'effettiva operatività in diverse parti dell'organizzazione - Può causare una limitata pubblicità negativa tale da influenzare le relazioni con altre organizzazioni o le relazioni con il pubblico - Coinvolge dati classificati come interni - Le modifiche non autorizzate, o la perdita di accuratezza, sono moderatamente critiche. L'impatto è notevole e comincia ad avere gravi ripercussioni sul business e le sue operazioni - La perdita di disponibilità può essere tollerata fino a una/due ore - Può causare la violazione di obblighi legali o normativi
Molto alto	- Può causare violazioni e ostacolare una eventuale attività investigativa - Può causare interruzioni gravi delle attività proprie dell'Organizzazione con ripercussioni consistenti anche in altre organizzazioni - Può impedire l'effettiva operatività dell'organizzazione - Può causare un'ampia pubblicità negativa tale da influenzare le relazioni con altre organizzazioni, con il pubblico o con altri paesi - Coinvolge dati classificati come Confidenziali - Le modifiche non autorizzate, o la perdita di accuratezza, sono fondamentali per i processi e leapplicazioni di business - Causa di perdite economiche elevate - Costituisce una violazione grave degli obblighi contrattuali relativi alla sicurezza delle informazioni fornita da terze parti - Può causare una violazione grave di obblighi legali o normativi
Critico	- Può causare violazioni eccezionalmente gravi - Può causare danni eccezionalmente gravi all'efficacia di attività operative o logistiche - Può causare interruzioni eccezionalmente gravi delle attività proprie dell'organizzazione con gravi ripercussioni anche in altre organizzazioni - Può impedire seriamente l'effettiva operatività dell'organizzazione, arrivando eventualmente acausarne la chiusura - Può causare un'ampia pubblicità negativa tale da influenzare negativamente le relazioni conaltre organizzazioni, con il pubblico o con altri Paesi - Coinvolge dati classificati come riservati
	- Le modifiche non autorizzate, o la perdita di accuratezza sono molto critiche. L'impatto è moltograve e le conseguenze possano portare al fallimento totale di alcuni o di tutti i processi/applicazione di business. - Gli asset coinvolti devono essere SEMPRE disponibili - Vi sono Interessi economici e commerciali di altissimo interesse per la concorrenza, di altissimovalore commerciale - Causa di perdite finanziarie eccezionalmente elevate - Costituisce una violazione eccezionalmente grave degli obblighi contrattuali relativi alla sicurezza delle informazioni fornita da terze parti - Può causare una violazione eccezionalmente grave di obblighi legali o normativi

6. Gestione degli eventi di sicurezza INFORMATICA

Gli incidenti vengono gestiti attraverso una sequenza di fasi distinte:

- preparazione all'incidente;
- rilevazione, identificazione e analisi;
- contenimento, eradicamento e recupero;
- attività post-incidente.

6.1. Attività pre-incidente

Le metodologie di risposta agli incidenti enfatizzano l'uso proattivo e continuo di strumenti, formazione e processi necessari per prevenire gli incidenti garantendo che sistemi, reti e applicazioni siano sufficientemente sicuri. La preparazione include tutte le attività che consentono di rispondere a un incidente:politiche, strumenti, procedure, efficaci piani di azione e comunicazione, e implica che i gruppi interessati abbiano istituito i controlli necessari per recuperare e continuare le operazioni dopo che un incidente è statoscoperto. Le analisi post-mortem di incidenti precedenti devono costituire la base per il miglioramento continuo.

6.2. Rilevazione, identificazione e analisi

I primi passi per rilevare, verificare, investigare e analizzare un incidente sono importanti per lo sviluppo di una strategia efficace di contenimento ed eradicazione. Una volta confermato un incidente, è possibile assegnare risorse per indagare l'ambito, l'impatto e la risposta necessari. Le fasi di rilevamento e analisi determinano la fonte dell'incidente e preservano le prove; tali informazioni devono essere comunicate agli amministratori di Sistema che detengono ed aggiornano il "Registro degli incidenti di sicurezza IT dell'Istituto".

6.3. Contenimento, eradicamento e recupero

Il contenimento è la fase di triage in cui il sistema o servizio compromesso viene identificato, isolato o comunque mitigato e quando le parti interessate vengono avvisate. Le procedure di contenimento tentano di limitare attivamente la portata e l'entità dell'attacco. Il contenimento implica l'acquisizione, la conservazione, la messa in sicurezza e la documentazione di tutte le prove. Il contenimento deve impedire ai dati di lasciare la rete attraverso le macchine interessate e impedire che l'attaccante causi ulteriori danni allerisorse aziendali. L'eradicazione è la rimozione di codice dannoso, o di un profilo o accesso inappropriato. L'eradicazione include anche la gestione delle vulnerabilità che potrebbero essere state la causa principale della compromissione.

6.4. Attività post-incidente

Tutte le attività di risposta agli incidenti saranno documentate e esaminate post-mortem per valutare se il processo di indagine è stato efficace. Successive correzioni possono essere apportate ai metodi e alle procedure utilizzate per migliorare il processo di risposta agli incidenti.

La documentazione offre l'opportunità di migliorare i processi di risposta agli incidenti e identificare problemi ricorrenti. Questa fase consente anche l'analisi dell'incidente per le sue implicazioni procedurali, la raccolta di metriche e l'incorporazione di buone pratiche nelle attività di risposta e formazione future.

Allegato 3 – Politica di gestione dei log

1. Scopo del documento

Lo scopo di questo documento è definire le tipologie di log da tenere e le regole di conservazione da applicare,in particolare evidenziando quali informazioni devono essere tracciate e per quanto tempo.

2. Ambito di applicazione

La politica descritta in questo documento si applica ai log dei sistemi informatici che forniscono servizi agli utenti dell'Istituto.

3. Necessità di conservazione dei log

La gestione dei log da parte dell'Istituto è necessaria, e verrà utilizzata, esclusivamente per assicurare il rispetto della normativa a tutela dei dati personali, poiché consente di ricostruire l'attività di un sistema informatico e individuare eventuali responsabilità in caso di errore, violazioni di legge e databreach (art. 33 comma 3 del Regolamento UE 2016/679). Il principio di responsabilità (art. 5 comma 2 del Regolamento UE 2016/679) introduce per la prima volta, l'obbligo, in capo al Titolare del trattamento, di dimostrare il rispetto della normativa decidendoautonomamente modalità, garanzie e limiti del trattamento dei dati personali, in considerazione del contesto operativo in cui ci si trova. Da una parte, quindi, i titolari del trattamento non solo devono compiere tutte leattività necessarie per la salvaguardia degli interessati, ma devono anche precostituirsi le prove degli adempimenti in caso di ispezioni da parte delle autorità competenti.

4. Persistenza dei log

I log devono essere conservati e mantenuti in modo appropriato per prevenire eventuali perdite di informazioni o la possibile compromissione da parte di intrusi. La conservazione dei log deve inoltrerispettare i requisiti normativi e fornire esclusivamente le informazioni necessarie per attività forensi e di risposta agli incidenti.

5. Correlazione dei log

I log devono essere gestiti in modo centralizzato e accessibili ai responsabili di settore e al responsabile di servizio per poter effettuare una correlazione anche automatizzata delle informazioni in essi contenuti. al fine di soddisfare i requisiti normativi e fornire le sufficienti informazioni necessarie per le attività forensi, di risposta agli incidenti e di analisi di databreach.

6. Stato di attuazione

I log attualmente tracciati sono quelli delle righe di colore verde

I dati di tracciamento a livello applicativo (evidenziali nella tabella sottostante in colore marrone), vanno conservati seguendo le disposizioni normative, applicando la cifratura, l'anonimizzazione, minimizzando i tempi di conservazione e dandone adeguata informativa agli interessati in osservanza delle disposizioni di legge e gli accordi sindacali; quindi, potranno essere implementati solo dopo aver compiuto tutti i passi succitati.

7. Tabella dei log

Categorie e tipologie	Cosa tracciare	Sistemi interessati	Tempo di conservazione	Norme di riferimento	Descrizione
Accesso amministratoridi sistema e profili privilegiati	• Username • Timestamp • Descrizione evento: Log-in,Log-out, Tentativi falliti • Sistema di elaborazione acceduto	• Sistemi operativi • Software complessi • Apparatidi rete	Min 6 mesi Max 2 anni	1. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 Gazzetta Ufficiale n. 300 del 24/12/2008 2. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016	1. *"…la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativodi accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivia sistemi di elaborazione o a sistemi software…"* (Log-in, log-out e tentativi falliti) 2. 5.5.1 Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa. N.B. gli Amministratoridi Sistema non devono poter accedere a tali log che devono avere caratteristiche di non modificabilità
Modifiche utenze amministrative	• Aggiunta utenti con privilegi amministrativi • Eliminazione utenti con privilegi amministrativi	• Sistemi operativi • Software complessi • Apparatidi rete	Min 1 anno Max 2 anni	Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016	*5.4.1 Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.*
Attività di amministratoridi sistema e profili privilegiati	• Username • Timestamp • Operazioni svolte	• Sistemi operativi • Software complessi	Min 1 mese Max 6 mesi	1. ISO 27001 2. Misure minime di sicurezza ICT per le Pubbliche	1. 12.4.3 Le attività degli amministratori e degli operatori devono essere sottoposte a log, e questi devono

		si			
	• Sistema di elaborazione acceduto			Amministrazioni,26 aprile 2016	essere protetti e riesaminati periodicamente. 2. 5.1.4 Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
Autenticazione e Single Sign Onper tutti i servizi web federati con il sistema di autenticazione dell'Istituto	• Timestamp • Username • Log-in, • Log-out • Servizio • IP	Server di autenticazione (LDAP, AD, Radius, Shibboleth, CAS etc.)	Min 1 mese Max 1 anno	1. Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007 2. Linee guida in materia di privacy eprotezione dei dati personali in ambito universitario del CODAU	1. *"…l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzionemediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni…"* 2. *"Tracciamento sistemistico e di rete Ricadono in questo ambito i dati di tracciamento generati da apparati di rete e componenti infrastrutturali."*
Navigazione web (attivabile a seguito di incidenti e su sottinsiemi specifici)	• IP sorgente • IP destinazione • Porta sorgente • Porta destinazione • Protocollo • URL visitato	Apparati che gestiscono l'accesso alla rete Internet (es.: Firewall, IPSetc.)	A seconda della finalità da perseguire	Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007	"…l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle

					informazioni…”
Operazioni server DHCP	• Associazione macaddress-IP • Associazione utente-mac	Sistemi peril rilascio automatico	Min 1 anno Max 2 anni	1. Misure minime di sicurezza ICT per le Pubbliche	*1.2.1 Implementare il “logging” delle operazioni del server DHCP.*
	address (conservata separatamente dall’associazione precedente)	degli indirizzi IP		Amministrazioni,26 aprile 2016 2. Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Accesso WIFI	• ID utente • Indirizzo IP e MAC address • Nome AP • Timestamp (inizio e fine sessione) • Tipo e versioneSO • Numero byte scambiati	Sistemi per l’accesso WIFI	Min 1 anno Max 2 anni	Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Accesso VPN	• ID utente (con eventuali ruoli di accesso alla rete) • Indirizzo IP (siaesterno che interno) • Timestamp	Concentratori VPN	Min 1 anno Max 2 anni	Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	

Eventi firewall, IPS e altri apparati di rete	Attivare moduli IPS del firewall	Apparati di controllo edi rete	Min 15 giorni Max 6 mesi	1. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni 26 aprile 2016 (classificazione standard) 2. ISO 27001	1. *8.1.3 Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.* 2. *13.1.1 Appropriate attività di logging e monitoraggio dovrebbero essere applicate per registrare e rilevare azioni che potrebbero avere un impatto sulla sicurezza delle informazioni*
Attività utente su repository di file	• Timestamp • Username • Hostname • Accesso ai file • Creazione file • Cancellazione file • Modifica file	Depositi centralizza tidei dati di Istituto (es.:File server, SharePoin t etc.)	Min 15 giorni Max 6 mesi	1. ISO 27001 2. Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34) 3. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016	1. *12.4.1 I log degli eventi che registrano le attività degli utenti, le eccezioni, i guasti e gli eventi di sicurezza delle informazioni dovrebbero essere prodotte, mantenute e regolarmente riesaminate.*
Utilizzo e gestione delle postazioni di lavoro	• Timestamp • Log-in, • Log-out • Username • Hostname • IP • Inventario dell'Hardwar ee del Software installato / utilizzato	• PDL • VDI	Min 6 mesi Max 1 anno	1. Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34) 2. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016 3. Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	

Accesso alle postazioni dei laboratori informatici	• Timestamp • Log-in, • Log-out • Username • Hostname • IP	Aule informatiche fisiche e virtuali	Min 6 mesi Max 1 anno	1. Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34) 2. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016 3. Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Applicazioni per richieste diintervento	• Anagrafica utente • Motivo ticket	Sistemi di gestione deiTicket	Min 1 anno dopo il dato viene anonimizzato	Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34)	
Utilizzo dei servizi di stampa	• Timestamp • Username • Hostname	Sistemi di stampa centralizzati	Min 1 anno dopo il dato viene anonimizzato	Regolamento Ue 2016/679 (art 5, art. 33 e art. 34)	
Registro degli incidenti	• Tipologia incidente • Veicolo • n. impattati • n. danneggiati • fonte segnalazione • note • Azioni di contenimento e ripristino • Riaperture caso • Responsabile attività malevola • Databreach • Notifica		Min 2 anni dopo il dato viene anonimizzato	Rispondere a una richiesta da parte delle autorità amministrativedi vigilanza, ispettive o giudiziarie competenti	

	garante • Notifica interessati				

Allegato 4 – Politica di gestione di filtro sul traffico di rete

1. Scopo del documento

Lo scopo di questo documento è definire una politica di filtraggio dei dati, dei servizi e delle risorse informatiche di cui l'Istituto è titolare, con l'intento di aumentare la sicurezza informatica e proteggere la privacy.

2. Ambito di applicazione

La politica descritta in questo documento si applica agli scambi di dati che avvengono tra le reti, i dispositivi,le applicazioni, i servizi dell'Istituto verso Internet e tra di loro, sulla rete interna o nel cloud. Ogni flusso di dati che parte o arriva a delle risorse informatiche dell'Istituto, siano esse interne o cloud, è potenzialmente soggetto alle politiche di filtro descritte in questo documento.

3. Filtri sui flussi di dati delle reti interne

Il traffico dati che entra ed esce dalla rete interna dell'Istituto viene filtrato per impedire l'accesso a risorse che possono veicolare Malware (es.: Ransomware, Botnet, DarkWeb, VPN anonime, SPAM URL, etc.), materiali illegali o inappropriati (es.: sostanze illecite, pornografia, estremismo, abusi, etc.), materiali copertidal diritto d'autore. Il traffico viene filtrato sulla base di categorie predefinite e database di risorse notoriamente malevole.

I filtri vengono applicati per il traffico proveniente sia dall'infrastruttura di rete fisica (cablata) che dall'infrastruttura di rete wireless (WiFi).

Di seguito la tabella delle categorie dei contenuti filtrati e le relative azioni perimetrali.

Categorie	Azioni
Adult/mature Content	
Abortion	Allow
Advocacy Organizations	Allow
Alcohol	Allow
Alternative Beliefs	Allow
Dating	Allow
Gambling	Allow
Lingerie and Swimsuit	Allow
Marijuana	Allow
Nudity and Risque	Allow
Other Adult Materials	Allow
Pornography	Block
Sex Education	Allow
Sports Hunting and War Games	Allow
Tobacco	Allow
Weapons (Sales)	Allow
Bandwidth Consuming	
File Sharing and Storage	Allow
Freeware and Software Downloads	Allow

Internet Radio and TV	Allow
Internet Telephony	Allow
Peer-to-peer File Sharing	Block
Streaming Media and Download	Allow
Potentially Liable	
Child Abuse	Block
Discrimination	Allow
Drug Abuse	Allow
Explicit Violence	Block
Extremist Groups	Block
Hacking	Allow
Illegal or Unethical	Allow
Plagiarism	Allow
Proxy Avoidance	Block
Security Risk	
Dynamic DNS	Block
Malicious Websites	Block
Newly Observed Domain	Warning
Newly Registered Domain	Warning
Phishing	Block
Spam URLs	Block
Unrated	Warning

Allow: azione permessa

Block: azione negata

Warning: l'utente viene avvisato, ma può decidere di proseguire