ISTITUTO COMPRENSIVO
"C. SALUTATI - A. CAVALCANTI"
Piazza A. Moro, 1 – 51011 Borgo a Buggiano (PT)
C.F.: 81003470473 - tel. 0572 - 32018
ptic81900g@istruzione.it – ptic81900g@pec.istruzione.it www.istitutosalutaticavalcanti.it

I.C.S. - "SALUTATI - CAVALCANTI"-BUGGIANO
Prot. 0002624 del 05/07/2023
III (Uscita)

MODELLO ORGANIZZATIVO GESTIONE IT

Sommario

1. SCOPO DELLE PROCEDURE

Le procedure di seguito indicate hanno l'obiettivo di descrivere le modalità operative adottate dal Titolare per consentire la gestione degli aspetti informatici all'interno della struttura, concordemente con il D.P.O..

Costituisce documento funzionale alla gestione delle procedure anche il Regolamento informatico interno adottato.

2. DEFINIZIONI

- ***Utente***: qualunque persona fisica cui sia stato attribuito un profilo di autorizzazione per l'accesso ai sistemi**.**
- ***Data Breach***: qualsivoglia violazione di dati personali o di informazioni gestite dal Titolare, che comporta, anche accidentalmente, la distruzione, la modifica, la rilevazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, memorizzati o comunque elaborati.
- **Amministratori di sistema o A.D.S.:** le figure professionali con le quali è in essere un contratto di lavoro dipendente o assimilabili ovvero un contratto di fornitura servizi IT con la Società, finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
- ***Prodotto/Software/Applicativo/Strumento***: programma o sistema informatico deputato al trattamento dei dati personali e/o che incide sulla sicurezza degli stessi;
- ***Privacy by Design***: la conformabilità alla G.D.P.R. delle misure tecniche, organizzative e di minimizzazione di trattamento dati effettuate con un prodotto;
- ***Privacy by Default***: la conformazione di un prodotto privacy by design rispetto al core delle attività svolte ed all'organizzazione.
- ***PbD***: Privacy by Design e Privacy by Default unitamente intesi

3. LE PROCEDURE

3.1 GESTIONE AMMINISTRATORI DEL SISTEMA INTERNI ED ESTERNI

Nell'Istituto è presente un solo Amministratore di Sistema, con qualifica di Responsabile sistemi informativi, i cui compiti sono riassunti di seguito:

a) Il Responsabile sistemi informativi annualmente (entro il 15 dicembre) provvede a verificare le liste degli account interni definiti per l'accesso ai Sistemi e Server, alle Applicazioni e alle Banche Dati in qualità di A.D.S.;

b) il Responsabile sistemi informativi annualmente, ed entro il mese di agosto, provvede a far verificare le liste degli account esterni definiti per l'accesso ai Sistemi e Server, alle Applicazioni e alle Banche Dati in qualità di A.D.S..

c) qualora il Responsabile sistemi informativi rilevi eventuali condotte non conformi che possano comportare responsabilità per il Titolare deve darne comunicazione al D.P.O. mediante invio mail sull'indirizzo dedicato;

d) il Responsabile sistemi informativi deve controllare eventuali cause sopravvenute di mancanza dei requisiti tecnici/personali/organizzativi in capo agli utenti del agli applicativi di Istituto.

e) entro il 15 dicembre di ogni anno, il Responsabile sistemi informativi deve predisporre la Relazione annuale sottoponendola alla sottoscrizione del Titolare. In tale Relazione deve emergere la valutazione da parte della F.S. AREA 2 – FORMAZIONE E INNOVAZIONE e dell'animatore digitale, degli eventi tecnici ed organizzativi che hanno interessato il sistema implementato in materia di A.D.S. A titolo esemplificativo il Responsabile sistemi informativi deve analizzare:

- ✓ eventi che hanno riguardato il sistema di loggatura;
- ✓ eventi di sicurezza; ecc.

Le analisi interne devono essere esaurite entro il mese di novembre di ogni anno.

- PREDISPOSIZIONE RELAZIONE ANNUALE
- COMUNICAZIONE AL D.P.O.

Il Responsabile sistemi informativi deve comunicare la documentazione prodotta al D.P.O. via mail all'indirizzo dedicato.

3.2 DATA BREACH

Un Utente deve comunicare un potenziale Data Breach al D.P.O. mediante invio all'indirizzo rpd.mail@istitutosalutaticavalcanti.it e in cc a ptic81900g@istruzione.it
Per Data Breach si intendono a titolo esemplificativo:

- Eventi correlati ad accesso di soggetti interni o esterni non autorizzati, ai dati personali oggetto di trattamento da parte del Titolare;
- Perdite o furti di supporti di memorizzazione non protetti che contengono dati personali;
- Attacchi informatici.

e tutti quegli eventi che possano esporre i dati personali a violazioni.

Per quanto di competenza, l'Utente nella comunicazione deve descrivere la violazione subita fornendo tutti gli elementi utili ed indicare i dati personali o le informazioni che ne siano stati oggetto, ossia:

✓ Descrizione della violazione (indicando le modalità con cui è venuto a conoscenza della violazione e comunque qualunque ogni altro elemento utile per circoscrivere la violazione);

✓ Natura e tipologia dei dati coinvolti nella violazione (indicando i sistemi violati, le tipologie di dati e/o informazioni e comunque ogni altro elemento utile).

L'Utente che ha segnalato l'eventuale Data Breach deve rimanere a disposizione del D.P.O. per eventuali chiarimenti in merito.

Il D.P.O. a fronte della segnalazione in accordo con il Responsabile Sviluppo ed Innovazione, pone in atto misure atte a scongiurare il sopraggiungere o l'aggravarsi di un rischio maggiore rispetto all'evento coinvolgendo eventuali fornitori.

Qualora il D.P.O. ritenga di classificare l'evento in un effettivo Data Breach, unitamente al Responsabile sistemi informativi compila la comunicazione all'Autorità di controllo, sottoponendola alla sottoscrizione del Titolare.

Il D.P.O. provvede ad inviare il documento di notificazione all'Autorità di Controllo entro 72 ore decorrenti dalla conoscenza del Data Breach.

Il D.P.O. verifica eventuali impatti sugli interessati, ed in caso positivo ne avverte il Titolare, proponendo modalità di messa a conoscenza della violazione degli interessati coinvolti. Spetta al Titolare decidere tale modalità ed autorizzare la comunicazione.

Il D.P.O. deve compilare il Registro delle Violazioni e allegare il Verbale di analisi del Data Breach.

3.3 IDENTITA' E PROFILI (Gestione Identità e Accesso ai sistemi)

Si rimanda al Regolamento per l'utilizzo della strumentazione informatica istituzionale e della rete internet per la tutela della privacy.

3.4 DISMISSIONE STRUMENTO DI MEMORIZZAZIONE

L'animatore digitale contatta l'Utente per concordare i termini di restituzione, e valutare le problematiche tecniche, decidere circa il reimpiego o la dismissione dello strumento riconsegnato dall'Utente.

Qualora l'animatore digitale decida di reimpiegare e riciclare lo strumento deve adottare misure adeguate deputate a prevenire accessi non consentiti alle informazioni eventualmente contenute. Tra esse esemplificativamente si segnalano.

- ✓ Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder);
- ✓ Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF);
- ✓ Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, nastri magnetici su bobine aperte o in cassette).

L'animatore digitale adotta tali misure anche in combinazione tra loro tenendo conto degli standard tecnici esistenti, e comunque verificare la non intellegibilità delle informazioni.

L'animatore digitale provvede a riassegnare lo strumento o comunque a metterlo a disposizione per la riassegnazione o riciclaggio.

Nel caso in cui tali attività vengano svolte tramite fornitori il Titolare del trattamento vincola questi ultimi a quanto sancito nell'Allegato CLAUSOLE RAAE – "Reimpiego o Riciclaggio".

3.5 SICUREZZA DEI DATI (PbD e sicurezza)

All'introduzione di un nuovo applicativo l'animatore digitale e il D.P.O., devono aggiornare la mappatura degli applicativi. L'animatore digitale dà notizia di ciò al Responsabile dei sistemi informativi.
Il Titolare del trattamento, sentita la Responsabile del trattamento, ed il D.P.O. devono valutare l'impatto privacy dell'applicativo preventivamente all'adozione ed allo svolgimento del trattamento. In particolare, dovranno verificare la coerenza del medesimo rispetto ai principi esercitabili dall'interessato ed alle misure di protezione inerenti i dati.

Al fine di dimostrare di aver effettuato una valutazione preventiva, dovranno integrare un apposito documento di analisi.

Qualora subentrino novità normative per integrazioni o modifiche dell'attuale G.D.P.R. piuttosto che provvedimento nazionali o europei correlati al tema informatico, il D.P.O. dovrà darne conoscenza al Titolare del trattamento per valutare unitamente come ciò possa eventualmente impattare sui sistemi e gli applicativi esistenti adoperandosi per pianificare eventuali azioni necessarie a conformarsi.