POLICY SICUREZZA INFORMATICA

APPLICAZIONI CLIENT/SERVER E WEB

PREMESSA

AXIOS Italia Service S.r.l. SU con sede in Via E. Filiberto 190 – 00185 Roma, P.IVA 06331261005 (di seguito AXIOS), da oltre 30 anni, sviluppa software per la gestione delle Segreterie Scolastiche nelle Scuole sia nell'utilizzo in locale (client/server) che su web.

Obiettivo principale dell'azienda, oltre quello di rendere agevole il lavoro quotidiano dei nostri clienti, è quello di garantire la sicurezza degli applicativi adeguandoli alle normative che si sono susseguite negli anni. Per questo motivo, AXIOS si è impegnata e ha ottenuto le certificazioni ISO 9001:2015, ISO 27001:2013, ISO 27018:2014 e ISO 27017:2015 per i seguenti campi applicativi: "Progettazione, sviluppo, manutenzione e assistenza di software gestionale e servizi SaaS connessi" ed inoltre, da aprile 2019, la qualifica AgID secondo la circolare n.3 del 9 aprile 2018 per gli applicativi SaaS.

Sono circa 3000 gli istituti scolastici che utilizzano con successo i nostri software. Questo ci obbliga e ci impegna quotidianamente nel miglioramento della qualità dei servizi offerti e ci responsabilizza riguardo la sicurezza dei dati trattati con i nostri applicativi/servizi.

Il 25 maggio 2018 è entrato in vigore il Regolamento UE 2016/679 (di seguito GDPR) sulla protezione dei dati che ha modificato in maniera sensibile l'approccio alla gestione, protezione e trattamento dei dati personali.

AXIOS, attraverso questo documento, intende dare evidenza delle misure di sicurezza adottate nel rispetto di quanto previsto dal GDPR e delle altre normative vigenti in merito al trattamento dei dati personali.

TIPOLOGIE DI DATI TRATTATI

Le differenti tipologie di software applicativi locali (client/server) e web comportano il trattamento di diverse tipologie di dati, appartenenti alle varie categorie di interessati (alunni, personale, famiglie, fornitori, etc.), a partire da quelli generici, fiscali, amministrativi fino a quelli riguardanti categorie di dati particolari (art.9 dell'RGDP - Trattamento di categorie particolari di dati personali) e Giudiziari (art.10 dell'RGDP – Trattamento dei dati personali relativi a condanne penali e reati).

SICUREZZA DEGLI APPLICATIVI CLIENT/SERVER

L'accesso da parte del personale dell'Istituto avviene attraverso credenziali di autenticazione (nome utente e password) assegnate ad ogni soggetto autorizzato. In caso di erroneo inserimento dei dati di accesso il software provvede, dopo il terzo tentativo, al blocco temporaneo dell'utenza ed all'invio di una mail di avvertimento all'indirizzo indicato all'interno della procedura di personalizzazione del cliente.

AXIOS fornisce ai propri clienti tutti gli strumenti necessari per salvaguardare il proprio patrimonio informativo, tra i quali backup automatico e backup su cloud, ma è sempre responsabilità dell'Istituto la sicurezza dei dati contenuti negli applicativi Client/Server (Es.: Backup e protezione da Virus informatici).

SICUREZZA DEGLI APPLICATIVI WEB

DISLOCAZIONE GEOGRAFICA DEI DATA CENTER

AXIOS si affida, per l'infrastruttura web, ad Aruba S.p.A. con sede legale in Via San Clemente n. 53, Ponte San Pietro (BG).

Aruba S.p.A. offre tutte le certificazioni relative ai servizi web quali tra le altre la ISO 9001:2015 – ISO 27001:2013 - ISO 14001:2015 - ANSI/TIA 942-A-2014.

Ulteriori informazioni sulle certificazioni di Aruba S.p.A. sono reperibili all'indirizzo web:

https://www.aruba.it/certificazioni.aspx

SICUREZZA DATA CENTER

I Data Center Aruba utilizzati da AXIOS sono dislocati esclusivamente in Italia e garantiscono elevati standard di sicurezza e protezione dei dati.
Nel dettaglio:

Data Center IT1:

- Rating 4 (former Tier 4) ANSI/TIA 942-B-2017
- GO - Garanzia d'Origine dell'energia (100% rinnovabile)
- ISO 9001 - Qualità dei servizi offerti
- ISO 27001 - Sicurezza IT
- ISO 50001 - Sistema di gestione dell'energia
- ISO/IEC 27017 - Controlli di sicurezza sul cloud
- ISO/IEC 27018 - Gestione dei dati personali sul cloud
- ISO/IEC 27035 - Gestione di eventi e incidenti di sicurezza

Ulteriori informazioni disponibili all'indirizzo https://www.cloud.it/infrastrutture/italia-dc-it1.aspx

Global Cloud Data Center IT3:

- Rating 4 (former Tier 4) ANSI/TIA 942-B-2017
- GO - Garanzia d'Origine dell'energia (100% rinnovabile)
- ISO 9001 - Qualità dei servizi offerti
- ISO 14001 - Sistema di gestione ambientale
- ISO 27001 - Sicurezza IT
- ISO 50001 - Sistema di gestione dell'energia
- ISO/IEC 27017 - Controlli di sicurezza sul cloud
- ISO/IEC 27018 - Gestione dei dati personali sul cloud
- ISO/IEC 27035 - Gestione di eventi e incidenti di sicurezza

Ulteriori informazioni disponibili all'indirizzo https://www.datacenter.it/data-center-aruba/italia-milano-dc-it3.aspx

SICUREZZA DELLE COMUNICAZIONI

L'accesso alle applicazioni web avviene mediante il protocollo SSL che garantisce un elevato livello di sicurezza in fase di utilizzo dei servizi in rete su internet. In particolare, AXIOS utilizza certificati aggiornati alla più recente e sicura versione di SSL disponibile.

DISPONIBILITA' DEI DATI

Disponibilità dei servizi – SLA 97%
Backup dei dati presenti nelle applicazioni web sono richiedibili mezzo PEC all'indirizzo: AXIOS@aziendemail.it e saranno resi disponibili entro 7 giorni dalla richiesta mediante appositi link con scadenza a 7 giorni.

GESTIONE E PROFILAZIONE UTENTI

Alla attivazione del servizio web, vengono create le credenziali per il SUPER UTENTE dell'Istituto. Il nome utente e la password provvisoria, da cambiare al primo accesso, vengono inviate mediante due mail distinte. Gli utenti delle applicazioni web sono gestiti direttamente dal Cliente attraverso il pannello di configurazione messo a sua disposizione che consente di creare gli utenti e di assegnare loro i profili di autorizzazione necessari.

GESTIONE UTENTI RELATIVAMENTE AGLI ACCESSI A SERVIZI DI TERZE PARTI

Con le credenziali per l'accesso ai servizi web, l'utente ha la possibilità di accedere ad ulteriori servizi opzionali erogati da fornitori con i quali il TITOLARE ha già attivo o ha intenzione di attivare un accordo/contratto di fornitura e ne ha abilitato o intende abilitare all'utilizzo gli utenti dal pannello di configurazione dei servizi stessi. I dati che vengono o verranno forniti ai fornitori dei servizi opzionali si riferiscono esclusivamente alle seguenti tipologie di dati personali: nome, cognome, indirizzo mail, ruolo (alunno, genitore, docente, ATA) e sono esclusivamente sotto la responsabilità del TITOLARE e del fornitore di servizi che agisce come RESPONSABILE del trattamento.

MODELLO DI RESPONSABILITA' CONDIVISA

Sicurezza e conformità sono una responsabilità condivisa tra AXIOS e il Cliente. AXIOS in qualità di fornitore è in grado di "progettare, sviluppare, manutenere e assistere software gestionale e servizi SaaS connessi" e si avvale di fornitori di servizi qualificati e certificati per l'implementazione dei propri prodotti/servizi.

Il "modello di responsabilità condivisa" evidenzia i livelli di responsabilità, nell'utilizzo e nella gestione dei servizi SaaS, che vengono condivisi tra AXIOS ed il Cliente. Ciò si rende necessario in quanto, generalmente ed erroneamente, il Cliente crede che utilizzando un servizio web (SaaS) siano demandate al fornitore tutte le responsabilità e le problematiche tecniche, di sicurezza e conformità normativa.

La tabella seguente rappresenta il "modello di responsabilità condivisa" tra AXIOS e i Clienti che si servono dei suoi prodotti/servizi:

Responsabilità	*SW locale (client/server)*	*Applicazioni web (SaaS)*
Dati (informazioni e documenti)	CLIENTE	CLIENTE
PC e mobile Device	CLIENTE	CLIENTE
Credenziali di accesso e autorizzazione	CLIENTE	CLIENTE
Applicativo	CLIENTE	AXIOS
Server e Infrastruttura di rete	CLIENTE	AXIOS

SICUREZZA DEI DATI E DEGLI APPLICATIVI WEB

CONTINUITA' OPERATIVA

La continuità operativa è garantita dalla presenza di numerosi Server dedicati all'erogazione dei servizi con ridondanze che garantiscono l'assenza di SPOF (Single Point of Failure).

AXIOS ha previsto anche un'infrastruttura secondaria presso il sito di Disaster Recovery, Datacenter Aruba IT3. Questa infrastruttura è progettata per ripristinare, in caso di disastro, un sottoinsieme selezionato dei sistemi primari.

BACKUP

I dati contenuti nei Server sono protetti da backup incrementali orari, giornalieri e settimanali con criteri di retention mirati a garantire il ripristino dei dati in tempi rapidi. Nello specifico:

Database Microsoft SQL Server:

- I cluster di database con la gestione dei dati sono tutti dotati di nodo passivo ed attivo in modalità Always-ON garantendo quindi sempre la continuità di servizio;
- Al sistema di log è stato dedicato un cluster apposito sempre configurato con nodo attivo e passivo;
- Per ogni database è garantito un Transaction Log Backup ogni 120 minuti con una retention di 7 giorni;
- Per i database Full Log è garantita una retention di 12 mesi

Storage:

- Relazione SnapMirror e SnapVault tra i due storage presenti in IT1 ed IT3;
- SnapMirror copia ogni ora i volumi primari, incluso lo snapshot, sullo storage secondario;
- Snapvault è utilizzato per trasferire sul Volume secondario uno snapshot al giorno con sette copie di retention;
- Le snapshot presenti sul volume primario sono:
    - Giornaliero: Backup giornaliero con 3 giorni di retention;
    - Snap_Voult con retention 24 ore, 2 giorni, 2 settimane
    - Mirror and Voult: 7 giorni, 52 settimane.

ARCHITETTURA INFORMATICA, MODALITA' DI GESTIONE DEI DATI E CONFIGURAZIONE

L'architettura informatica scelta da AXIOS per gli applicativi web è studiata per garantire continuità operativa, sicurezza dei dati e fluidità nell'utilizzo quotidiano.

La configurazione e la gestione dei Server presenti nell'infrastruttura sono svolte da personale qualificato di Aruba S.p.A.

Gli accessi ai Server da parte del personale AXIOS vengono eseguiti esclusivamente attraverso utenze di dominio personali al fine di poterne monitorare gli accessi.

Il personale AXIOS abilitato alla gestione dei Server è autorizzato al trattamento dei dati personali ai sensi dell'art.2-quaterdecies del D.lgs.196/03 così come modificato dal D.lgs.101/18, istruito sulle modalità di utilizzo e protezione dei dati nonché sulle procedure di sicurezza dei sistemi informatici e nominato Amministratore di Sistema (rif. provvedimento del Garante Privacy del 27/11/2008 poi modificato dal provvedimento del 25 giugno 2009).

I log degli accessi degli amministratori di sistema vengo conservati per non meno di 6 mesi e l'operato di questi ultimi è sottoposto a controllo annuale.

Ove si rendesse necessario l'accesso ai dati da parte di soggetti in outsourcing AXIOS provvederà a nominarli responsabili del trattamento ai sensi dell'art.28 dell'RGPD dopo essersi assicurata che gli stessi offrano adeguate garanzie in merito al trattamento dei dati personali (art.28 par.4 dell'RGDP).

Periodicamente vengono svolte, con l'ausilio di società specializzate, attività di Penetration test e Vulnerability Assessment con l'obiettivo di verificare l'efficacia e l'efficienza del sistema di protezione dei dati.

TRACCIABILITA' DEGLI ACCESSI UTENTE

AXIOS, per motivi di sicurezza, conserva per 18 mesi i log di accesso agli applicativi da parte degli utenti nonché i log relativi alle operazioni svolte dagli stessi.

Ove si rendesse necessario per esigenze tecniche, per motivi di sicurezza, per obblighi di legge o per ottemperare ad una eventuale richiesta dell'autorità giudiziaria, AXIOS si riserva di conservare i log per un periodo di tempo superiore e, se necessario, consegnarli alle autorità competenti.

I log di accesso agli applicativi da parte degli utenti sono resi disponibili su espressa richiesta del Dirigente Scolastico o dell'Autorità Giudiziaria secondo diverse modalità.

COMPLIANCE ALLE LINEE GUIDA AGID

AXIOS è qualificata AGID per quanto riguarda i servizi SaaS (es. Registro Elettronico, Segreteria Digitale, etc.). Relativamente agli applicativi client/server, AXIOS mette a disposizione degli Istituti il documento: "AXIOS_misure_minime" in riferimento alla Circolare AGID del 26 Aprile 2016 in materia di "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" per chiarire in che modo AXIOS e conforme e fornire indicazioni utili alla conformità degli Istituti stessi; il documento è scaricabile dal sito web www.axiositalia.it

PROTEZIONE DEI DATI PERSONALI

AXIOS Italia eroga i servizi nel rispetto della normativa che regola il trattamento dei dati personali agendo come Responsabile del trattamento ai sensi dell'art.28 del Regolamento UE 2016/679 (rif. documento DPA AXIOS Italia Service Srl).

NOMINA DI UN RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI (RPD/DPO)

AXIOS ha designato quale Responsabile della Protezione dei Dati (RPD-DPO) il Sig. Vincenzo De Vita raggiungibile all'indirizzo dpo@axiositalia.com

RESTITUZIONE E CANCELLAZIONE DEI DATI

In caso di mancato rinnovo del contratto in essere con l'Istituto scolastico, AXIOS garantisce la restituzione dei dati come previsto dall'art. 28 par. 3 lettera g. dell'RGDP attraverso le seguenti modalità:

- **Modalità di esportazione in formato intelligibile dei dati contenuti nei database locali (Software Client/Server)**
  Su espressa richiesta dell'Istituto, da esercitare attraverso PEC all'indirizzo axios@aziendemail.it o raccomandata entro 30 gg. dal mancato rinnovo del contratto, AXIOS Italia Service S.r.l. fornirà le istruzioni necessarie all'esportazione dei dati per i Software Client/Server.
- **Modalità di restituzione in formato intelligibile dei dati contenuti nei database web**
  Su espressa richiesta dell'Istituto, da esercitare attraverso PEC all'indirizzo axios@aziendemail.it o raccomandata entro 30 gg. dal mancato rinnovo del contratto, AXIOS Italia Service S.r.l. fornirà i dati contenuti in cloud in formato CSV, JSON, XML intelligibile. Tale servizio verrà garantito attraverso

piattaforma dedicata predisposta da AXIOS dalla quale il cliente potrà prelevare i dati protetti da crittografia e da password di accesso. Le credenziali saranno fornite al cliente attraverso PEC o altro mezzo sicuro.
Si provvederà, successivamente, alla cancellazione dei dati (art.28 par.3 lettera g) o, in cambio di un canone annuo da definire in base alla quantità di dati da conservare, al mantenimento degli stessi.

AGGIORNAMENTO DEL DOCUMENTO

Il documento è liberamente scaricabile dal sito www.axiositalia.it nella sezione LEGALE e verrà aggiornato periodicamente ogniqualvolta ci dovessero essere revisioni in merito ai sistemi di sicurezza e continuità operativa dei sistemi cui si riferisce.

In caso di aggiornamento del documento verrà data comunicazione ai Clienti mezzo mail e sul portale AXIOS Scuola Digitale.

Roma, 29/09/2022

ELEONORA
IOMMI
29.09.2022
10:28:51
GMT+01:00