Conformità Piattaforma Eligo rispetto a: "*Allegato tecnico - Requisiti tecnico-organizzativi per la gestione digitale degli organi collegiali e delle operazioni di voto nelle istituzioni scolastiche*"

Il presente documento è redatto per dare riscontro all'"*Allegato tecnico relativo ai requisiti tecnico-organizzativi per la gestione digitale degli organi collegiali e delle operazioni di voto nelle istituzioni scolastiche destinate allo svolgimento a distanza alle attività di cui al comma 3, lett. a) e b) dell'articolo 44 del CCNL 2019/2021 che rivestono carattere deliberativo*". L'obiettivo del presente elaborato è fornire gli elementi che verifichino la **conformità della piattaforma** di voto Eligo rispetto ai requisiti richiesti per lo svolgimento a distanza di attività collegiali deliberative, con particolare attenzione a identificazione, autenticazione, sicurezza, segretezza del voto, documentazione degli esiti e protezione dei dati personali.

Contenuti:

1. Oggetto, finalità e riferimenti normativi

La piattaforma Eligo è un sistema di e-voting web based, erogato in modalità cloud, progettato per la gestione digitale di processi di voto, consultazione, elezione e deliberazione, incluse assemblee, organi collegiali, procedimenti elettivi e votazioni formalmente rilevanti. La piattaforma può essere adottata in contesti full remote, ibridi o in presenza assistita, mantenendo una gestione centralizzata delle regole di voto, delle autorizzazioni, delle evidenze e della reportistica.

Eligo opera nel mercato del voto elettronico e online dal 2005, con una presenza consolidata in Italia e con progetti attivati anche in contesti internazionali ed esteri. La piattaforma ha gestito oltre 20 milioni di votanti, 45.000 clienti e 55.000 elezioni e assemblee amministrate, a conferma di una scala operativa molto elevata.

La piattaforma è sviluppata e gestita in coerenza con il quadro normativo richiamato dall'Allegato tecnico, inclusi il Codice dell'Amministrazione Digitale, il Regolamento (UE) 2016/679, il D.Lgs. 196/2003, il D.Lgs. 33/2013, il D.P.R. 275/1999, le Linee guida AgID in materia di sicurezza, identità digitale, formazione, gestione e conservazione dei documenti informatici, nonché le regole tecniche e le prassi applicabili in materia di voto elettronico e trattamento dei dati.

Sotto il profilo delle verifiche esterne e della tenuta giuridica del modello di voto sono intervenuti i seguenti riscontri e pronunciamenti:

- **Garante per la protezione dei dati personali – 2011**. Nella vigenza e in base al contenuto dell'allora D.Lgs. 196/2003, così si è espresso il Garante per la protezione dei dati personali nel provvedimento conclusivo dell'istruttoria: "l'eventuale relazione tra elettori e preferenze di voto espresse non è registrata in alcuna tabella, né è ricostruibile partendo dalle informazioni archiviate nei database"; "La comunicazione elettronica avviene tramite protocolli crittografici"; "le misure descritte da IDTechnology si valutano adeguate per impedire l'identificazione diretta e indiretta dei votanti e dei voti espressi".

- **Tribunale di Roma – Sez. I – 2014**: "Le misure di sicurezza implementate hanno garantito che nessun elettore potesse votare più volte o produrre voti non conformi."

- **Tribunale Ordinario di Roma – 2015**: "Risultano approntate una serie di cautele tecnologiche idonee ad impedire un uso scorretto o improprio del voto e ad offrire le maggiori garanzie di riservatezza, segretezza e libertà di espressione del voto".

- **Tribunale Ordinario di Roma – 2021**: "Sono stati depositati atti [...] dai quali emerge che la piattaforma per il voto elettronico predisposta dalla Eligo Evoting & Consulting risulta idonea a garantire la personalità, libertà e segretezza del voto. [...] Inoltre, il rischio di possibili sottrazioni delle password ovvero di possibili accessi di "Pirati informatici" nel sistema elettronico è in astratto possibile, ma si rientrerebbe in ipotesi patologiche che non possono essere eliminate del tutto neanche in caso di voto esclusivamente cataceo".

- **Tribunale di Torino – 2025**: 'Le misure di sicurezza implementate hanno garantito che nessun elettore potesse votare più volte o produrre voti non conformi."

La piattaforma è inoltre progettata in linea con i principi europei applicabili ai sistemi di voto elettronico e internet voting, inclusi quelli espressi nella Raccomandazione del Consiglio d'Europa Rec(2017)5 sui sistemi di voto elettronico e nei relativi addendum e documenti applicativi successivi, con particolare riguardo ai principi di affidabilità, trasparenza, sicurezza, auditabilità, verificabilità, responsabilizzazione, tutela dell'elettore e segretezza del voto.

Le certificazioni possedute costituiscono evidenza documentale, verificabile presso gli enti certificatori, dell'adeguatezza dei presidi organizzativi e tecnici adottati e concorrono a qualificare la piattaforma come sistema idoneo ai sensi dei requisiti dell'Allegato tecnico.

In particolare, di seguito le certificazioni:

- **ISO 9001** — Sistema di gestione per la qualità, a presidio della definizione, del controllo e del miglioramento continuo dei processi aziendali e di erogazione del servizio.

- **ISO/IEC 27001** — Sistema di gestione per la sicurezza delle informazioni (SGSI), a garanzia della gestione strutturata dei rischi, dei controlli di sicurezza e della protezione della riservatezza, integrità e disponibilità dei dati; costituisce il riferimento diretto per i requisiti di sicurezza informatica di cui alla sezione dedicata del presente documento.

- **ISO/IEC 27017** — Controlli di sicurezza specifici per i servizi cloud, coerenti con la natura web

based e cloud della piattaforma.

- **ISO/IEC 27018** — Protezione dei dati personali (PII) trattati nei servizi cloud pubblici, a supporto degli obblighi in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679.

A completamento del profilo di qualificazione, IDTechnology S.r.l. è registrata al portale dell'Agenzia per la Cybersicurezza Nazionale (ACN) per i servizi qualificati ed è presente sul Mercato Elettronico della Pubblica Amministrazione (MEPA), elementi che agevolano i processi di affidamento, la qualificazione del fornitore e la verifica preliminare da parte delle amministrazioni utilizzatrici. Nel loro insieme, tali certificazioni e qualificazioni forniscono all'istituzione scolastica un riscontro oggettivo e verificabile a supporto della verifica di conformità di cui alla sezione seguente.

Nel perimetro di tali riferimenti, la piattaforma è concepita per garantire che ogni soluzione adottata dall'istituzione scolastica possa essere ricondotta a un impianto documentabile e verificabile, anche quando siano previste configurazioni differenziate per voto palese, voto segreto, quorum costitutivi e deliberativi, categorie di elettori o regole di accesso diversificate.

2. Principi di base

I principi fondamentali alla base della piattaforma sono sintetizzabili come segue:

- La piattaforma garantisce l'**identificazione certa degli aventi diritto** attraverso identità digitali univoche, non condivise e sempre riconducibili al singolo soggetto abilitato. La piattaforma prevede l'accesso tramite SPID, CIE, autenticazione tramite credenziali d'accesso univoche fornite via email con supporto di autenticazione forte con doppio fattore di autenticazione (MFA), con modalità OTP via SMS. Infine è anche possibile l'integrazione ad aree riservate tramite SSO (Single Sing On).
- La piattaforma assicura la **validità formale del processo** attraverso la produzione di evidenze tecniche, registri di operazione, report di scrutinio e documentazione finale con firma digitale e marcatura temporale, così da garantire integrità, opponibilità e stabilità del risultato nel tempo.

- La piattaforma protegge il voto attraverso più **livelli di sicurezza**: comunicazione HTTPS/TLS, cifratura applicativa, cifratura del dato a riposo, segregazione dei ruoli e degli ambienti, logging, audit e controllo degli accessi.
- La preferenza di voto, nei casi di voto segreto, è **anonimizzata e cifrata direttamente sul client del votante mediante crittografia asimmetrica a 2048 bit** (che può arrivare a 3072 bit), prima della trasmissione al sistema, così da impedire la ricostruzione del legame tra identità e voto anche all'interno dell'infrastruttura applicativa.
- La piattaforma può inoltre, opzionalmente, adottare **protocolli crittografici avanzati** di tipo end-to-end per supportare modelli di voto a bassa coercizione e scenari di verificabilità universale e individuale, mediante ricevute crittografiche di voto, hash di verifica rilasciati all'elettore e bulletin board dedicata per il controllo pubblico della correttezza dello scrutinio, senza compromettere la segretezza della singola preferenza.

3. Requisiti di identificazione, autenticazione e accesso

3.1 Identificazione degli utenti

La piattaforma garantisce un'**identificazione univoca degli utenti** attraverso un modello di identity management via **SPID e CIE** che consente di associare ogni accesso a uno specifico avente diritto o utenti amministrativi e di sorveglianza. Ogni elettore, componente dell'organo collegiale, presidente, segretario verbalizzante o operatore autorizzato accede mediante identità individuale non condivisa, definita all'interno del registro degli aventi diritto o federata tramite sistemi esterni di autenticazione.

La piattaforma permette di associare l'identità autenticata alla posizione dell'utente nel procedimento, verificando il relativo diritto di accesso e di voto. **Il controllo può essere effettuato su base anagrafica, per appartenenza a gruppo o categoria, per ruolo, per lista elettorale, per collegio, per sede oppure per appartenenza a uno specifico organo o sottoinsieme dell'organo collegiale. In questo modo l'accesso non è soltanto identificato, ma anche qualificato rispetto ai diritti effettivamente esercitabili.**

In tutti i casi, la piattaforma consente di verificare in modo preventivo la presenza del soggetto nel registro elettorale o nell'elenco degli aventi diritto, così da escludere accessi non autorizzati

e ridurre il rischio di errori di configurazione.

La piattaforma supporta anche flussi con registrazione chiusa. In tali scenari, qualora l'ente non disponga ancora dei dati di contatto degli aventi diritto per la consegna delle credenziali e non ci sia la possibilità di operare con SPID/CIE è possibile predisporre un form pubblico di registrazione attraverso il quale l'utente inserisce i propri dati e i propri contatti. A seguito della compilazione, l'utente riceve le credenziali di accesso o il DAL (Direct Access Link) sui recapiti dichiarati; tuttavia, l'abilitazione finale è subordinata alla verifica della presenza dell'elettore nel registro elettorale associato a quelle specifiche elezioni. In questo modo il processo di onboarding resta aperto alla raccolta delle informazioni mancanti, ma la registrazione è chiusa sotto il profilo dell'effettiva eleggibilità, che viene sempre verificata rispetto al registro elettorale configurato in piattaforma.

Per i contesti deliberativi scolastici, ciò significa che l'istituzione può configurare con precisione chi può accedere, chi può visualizzare i materiali, chi può votare, chi può osservare l'andamento del procedimento e chi può assumere funzioni di presidenza o verbalizzazione, mantenendo distinta la posizione di ciascun soggetto.

3.2 Autenticazione

La piattaforma adotta un modello di autenticazione parametrico e multilivello, calibrabile in funzione del tipo di votazione, del numero di elettori, della sensibilità del procedimento e del livello di garanzia richiesto. L'accesso può essere basato su credenziali individuali, su identità federate, su link di accesso controllato o su sistemi di identità digitale nazionale, sempre in combinazione con controlli di validità temporale e di pertinenza rispetto all'evento aperto.

Il sistema supporta diverse modalità di identificazione, configurabili in base al contesto organizzativo. Tra queste rientrano:

- l'accesso con **SPID e CIE**
- l'utilizzo di credenziali individuali recapitate via e-mail sotto forma di DAL (Direct Access Link) univoco e cifrato
- l'adozione di meccanismi di autenticazione rafforzata con secondo fattore OTP via SMS
- l'integrazione con sistemi *Single Sign-On* mediante SAML 2.0 e OpenID Connect

Questa flessibilità consente di adattare il livello di *assurance* al rischio del procedimento e alla natura dell'organo collegiale.

L'autenticazione è inoltre integrata con i **controlli applicativi di eleggibilità**. Ciò significa che il fatto di essere autenticati non comporta automaticamente il diritto a votare o a visualizzare ogni sezione della piattaforma: il sistema verifica anche il ruolo, il profilo, l'appartenenza al corretto gruppo elettorale, la finestra temporale di apertura del voto e l'effettiva abilitazione alla specifica scheda o seduta. In questo modo la piattaforma separa correttamente il controllo di identità dal controllo di autorizzazione.

3.3 Autorizzazioni e gestione dei ruoli

La piattaforma implementa un **modello di Role-Based Access Control a livello applicativo, costruito secondo il principio del minimo privilegio**. Ogni ruolo dispone esclusivamente delle funzioni necessarie rispetto alle attività da svolgere, con una separazione chiara tra area di voto, area di monitoraggio, area amministrativa, configurazione eventi, scrutinio e reportistica.

Il sistema consente di attribuire permessi diversi a profili quali amministratore di tenant (Area elettorale dell'ente), gestore dell'evento, osservatore, accreditatore, scrutatore, presidente, segretario verbalizzante ed elettore. Tale segmentazione permette di assegnare visibilità e capacità operative differenziate, evitando che un utente possa accedere a funzionalità eccedenti rispetto al proprio ruolo.

Le autorizzazioni possono essere configurate per singolo evento o per singola area elettorale. Ciò consente, ad esempio, di permettere ad un osservatore di visualizzare esclusivamente l'affluenza senza accesso ai risultati, oppure a un segretario di scaricare la reportistica finale senza poter modificare la configurazione del voto.

Ogni operazione amministrativa rilevante viene registrata nei **log applicativi** e può essere ricondotta al soggetto che l'ha eseguita. In questo modo la piattaforma supporta esigenze di accountability, audit interno, verifica ex post e gestione di contestazioni o richieste istruttorie.

3.4 Gestione delle sessioni

La piattaforma gestisce le sessioni utente con controlli specifici di sicurezza e coerenza del

flusso applicativo. **Ogni sessione è associata a uno stato verificato lato server, così da impedire salti di fase, riuso improprio della navigazione del browser o alterazioni client-side del percorso di voto.**

La piattaforma applica controlli di sicurezza sulle credenziali e sulle sessioni, inclusi lockout su tentativi errati, finestre temporali di osservazione, durata limitata delle sessioni, scadenza o invalidazione delle password quando previsto dal processo, e restrizioni che impediscono l'uso abusivo o ripetuto delle stesse credenziali. Tali controlli riducono il rischio di impersonificazione, di forza bruta e di riutilizzo improprio delle sessioni attive.

Per le operazioni di voto, sia palese sia segreto, e più in generale per tutte le attività sensibili del procedimento, la piattaforma applica meccanismi di mutua esclusione con locking distribuito, così da impedire che lo stesso soggetto esprima contemporaneamente il voto da più sessioni, dispositivi o browser. Il risultato è una gestione della sessione orientata non solo alla sicurezza dell'accesso, ma anche all'integrità dell'atto di voto.

4. Requisiti delle operazioni di voto

4.1 Requisiti generali

La piattaforma è progettata per garantire che ogni avente diritto possa esprimere il voto una sola volta per ciascuna scheda per la quale risulti abilitato. L'univocità del voto è assicurata attraverso un registro elettorale elettronico separato rispetto all'archivio delle preferenze espresse, nel quale viene registrato in modo non modificabile il fatto che l'elettore abbia esercitato il proprio diritto di voto.

Ogni voto validamente espresso viene sottoposto a controlli di coerenza formale, vincoli di selezione, verifiche di appartenenza alla corretta scheda e validazione delle condizioni operative previste dalla configurazione. Solo le espressioni conformi vengono considerate nello scrutinio finale, mentre eventi anomali, tentativi duplicati o stati incoerenti sono intercettati e bloccati dal sistema.

4.2 Voto palese

Nel caso di voto palese, la piattaforma consente di associare in modo certo l'identità del votante

alla scelta espressa, mettendo a disposizione dell'amministrazione o degli organi legittimati le evidenze necessarie alla verbalizzazione e alla conservazione. **Il risultato è quindi pienamente tracciabile, verificabile e riportabile nella documentazione finale della seduta.**

La piattaforma produce report di scrutinio e documenti riepilogativi idonei a rappresentare l'esito del voto, le presenze, l'affluenza e, ove previsto, il dettaglio delle espressioni di voto. Tali documenti possono essere sottoposti a firma digitale e marcatura temporale, così da rafforzarne autenticità, integrità e valore probatorio.

Questa modalità risulta adatta alle deliberazioni per le quali il regolamento dell'istituzione scolastica richiede la riconducibilità dell'espressione di voto al singolo componente, come tipicamente accade nelle votazioni palesi degli organi collegiali.

4.3 Voto a scrutinio segreto

Nel caso di voto segreto, la piattaforma adotta un modello tecnico volto ad impedire la ricostruzione del legame tra identità dell'elettore e preferenza espressa. La garanzia di segretezza si fonda su una pluralità di misure concorrenti: **separazione tra autenticazione e trattamento della preferenza, anonimizzazione del voto, cifratura sul dispositivo del votante, segregazione logica dei dati, assenza di un archivio che contenga in chiaro la coppia identità-voto, e controlli sui log e sui metadati per evitare forme di re-identificazione indiretta.**

La preferenza viene cifrata lato client prima della trasmissione e non è trattata come dato in chiaro nei componenti applicativi che gestiscono il solo flusso di accesso o di abilitazione. Il sistema registra che il soggetto ha votato, ma non conserva in forma riconducibile il contenuto della preferenza all'interno del registro dell'elettore. In questo modo il dato di partecipazione e il dato di scelta rimangono separati sia funzionalmente sia logicamente.

La piattaforma integra, inoltre, misure di hardening organizzativo e applicativo: limitazione dei privilegi degli operatori, segregazione dei ruoli amministrativi, audit dei processi, protezione dei database, cifratura dei backup e tracciamento degli accessi alle sole componenti tecniche autorizzate. La combinazione di queste misure minimizza il rischio che un amministratore, un fornitore di infrastruttura o un soggetto non autorizzato possa ricostruire il voto individuale.

5. Sicurezza informatica

La piattaforma adotta un modello di sicurezza multilivello che copre trasmissione, elaborazione, conservazione, monitoraggio e continuità operativa. Le comunicazioni avvengono su protocollo **HTTPS/TLS con certificati validi; i dati sono protetti con cifratura applicativa e con ulteriori meccanismi di cifratura at rest sui database, sui backup e sui log.**

Le preferenze di voto, nei flussi di voto segreto, sono cifrate direttamente sul dispositivo del votante mediante crittografia asimmetrica a 2048 bit (fino a 3072 bit). A questo livello si affiancano ulteriori misure di protezione quali RBAC, segregazione degli ambienti, WAF, protezione perimetrale, logging centralizzato, monitoraggio delle anomalie, vulnerability assessment, penetration test periodici, backup cifrati, disaster recovery e processi di change management e patch management.

Il gateway applicativo gestisce le richieste HTTP e HTTPS in entrata, ne convalida la legittimità tramite un **web application firewall** (WAF) integrato con l'obiettivo di mitigare nativamente gli attacchi DDoS e le minacce maligne (prevenzione delle intrusioni, SQL Injection). In particolare, la piattaforma protegge automaticamente dalle minacce provenienti dalla rete, rilevando e controllando il traffico in base ai profili di comportamento degli attacchi.

L'infrastruttura cloud è progettata per garantire resilienza, continuità del servizio e protezione fisica e logica delle risorse. Sono previste ridondanza geografica, replica dei dati, controllo degli accessi amministrativi, sistemi di alerting e metriche di monitoraggio delle componenti applicative e infrastrutturali. I dati rimangono sempre in data center fisicamente in Europa.

6. Protezione dei dati personali

La piattaforma è progettata secondo i **principi di privacy by design e privacy by default**. Il trattamento dei dati è limitato alle finalità strettamente necessarie alla gestione dell'evento elettorale o deliberativo, con particolare attenzione a minimizzazione, riservatezza, integrità, accountability e limitazione della conservazione.

Nel modello di erogazione della piattaforma sono previsti i presidi tipici dei rapporti tra titolare e responsabile del trattamento, con definizione delle finalità, delle categorie di dati, delle misure di

sicurezza, dei tempi di conservazione, delle modalità di cancellazione o restituzione e delle eventuali catene di sub-responsabilità. Il sistema supporta inoltre processi di esportazione, portabilità e cancellazione coerenti con gli obblighi privacy applicabili.

7. Formazione, gestione e conservazione dei documenti

La piattaforma mette a disposizione reportistica strutturata, documenti riepilogativi, export dei risultati, file di scrutinio certificati e registrazioni degli eventi di sistema utili alla verbalizzazione e alla ricostruzione del procedimento. I documenti generati possono essere prodotti in formati standard, stampabili ed esportabili, e possono essere sottoposti a firma digitale e marcatura temporale.

Questo consente di integrare la piattaforma con il ciclo documentale dell'istituzione scolastica, supportando protocollazione, fascicolazione, conservazione e successiva esibizione delle evidenze amministrative. Le informazioni possono essere organizzate in modo coerente con i requisiti di completezza, autenticità, integrità, leggibilità e reperibilità richiesti dalle regole in materia di documenti informatici.

Laddove il procedimento richieda verbalizzazione formale, la piattaforma fornisce gli elementi tecnici utili a documentare partecipazione, quorum, esiti, eventuali schede bianche o nulle, tempistiche dell'evento, stato di scrutinio e dati di monitoraggio coerenti con il livello di visibilità autorizzato.

8. Requisiti organizzativi e responsabilità

La piattaforma è concepita per inserirsi in un perimetro organizzativo chiaramente definito dall'ente utilizzatore. In ambito scolastico ciò richiede l'adeguamento dei regolamenti interni in materia di sedute a distanza, convocazione, verifica del quorum, modalità di voto, verbalizzazione e gestione di eventuali incidenti o malfunzionamenti.

Dal punto di vista applicativo, il sistema consente di **distinguere ruoli e responsabilità operative**, attribuendo a ciascun soggetto soltanto le funzioni pertinenti. È quindi possibile configurare presidenza della seduta, segreteria verbalizzante, ruoli di supporto tecnico, observer, scrutatori e amministratori, mantenendo separati i rispettivi ambiti di intervento.

La piattaforma supporta inoltre procedure di apertura e chiusura programmata degli eventi, gestione delle finestre temporali di voto, pubblicazione dei risultati finali, download della reportistica e, ove necessario, sospensione o riconfigurazione delle operazioni secondo quanto previsto dalle regole organizzative definite dall'istituzione.

9. Verifica di conformità

La piattaforma Eligo presenta caratteristiche tecniche, organizzative e documentali coerenti con i requisiti richiesti per la gestione digitale delle attività deliberative e delle operazioni di voto degli organi collegiali scolastici. In particolare, risultano presidiate le aree relative a identificazione degli aventi diritto, autenticazione, controllo degli accessi, univocità del voto, segretezza dello scrutinio, sicurezza informatica, protezione dei dati personali, tracciabilità del procedimento e produzione di evidenze documentali.

Per il voto palese, la piattaforma offre un livello pieno di tracciabilità e documentabilità del risultato. Per il voto segreto, la piattaforma mette a disposizione un modello tecnico idoneo a garantire separazione tra identità e preferenza, cifratura lato client, non riconducibilità del voto all'elettore e, se richiesto, strumenti avanzati di verificabilità crittografica dell'esito complessivo.

La piattaforma Eligo, in relazione ai requisiti tecnico-organizzativi per la gestione digitale degli organi collegiali e delle operazioni di voto nelle istituzioni scolastiche, è idonea a supportare processi deliberativi e di voto digitale segreto e palese in coerenza con i principi di sicurezza, anonimità, identificazione certa, autenticazione adeguata, integrità del procedimento, sicurezza informatica, protezione dei dati personali, tracciabilità delle operazioni e documentabilità degli esiti.

L'utilizzo nel contesto scolastico richiede la corretta configurazione del servizio e il suo inserimento nel quadro regolamentare, documentale e privacy dell'istituzione scolastica. In tale perimetro, la piattaforma costituisce una soluzione tecnicamente adeguata per lo svolgimento digitale delle attività collegiali e delle operazioni di voto con rilevanza deliberativa.