Prot. n. 5418/B1 del 28/10/2026

CONSIGLIO DI AMMINISTRAZIONE

VERBALE N. 9 DEL 28/10/2026

Oggi, in data 28 ottobre 2026, alle ore 16.00, si riunisce in modalità mista, ossia presso la sede dell'Istituto Superiore per le Industrie Artistiche di Firenze il Consiglio di Amministrazione e per via telematica tramite piattaforma Google Meet presso il link https://meet.google.com/rqo-bphi-uwe ovvero tramite collegamento telefonico al numero +1 404-850-0050 PIN: 658 351 892#, a seguito a convocazione prot. n. 5016/B1 del 26/10/2026, spedita dal Direttore Amministrativo, per conto del Presidente, alla casella mail dedicata consiglio.amministrazione@isiadesign.fi.it, il Consiglio di Amministrazione dell'ISIA di Firenze.

Risultano presenti:

		PRESENTI	ASSENTI
1 Arch. Massimiliano Morlacci	Presidente	x	
2 Prof. Simone Paternich	Direttore	x	
3 Avv. Aldo Fittante	Rappresentante Esperto MUR		x
4 Prof. Marco Tognetti	Rappresentante Docenti	x	

5 Sig.ra Hoda Aboulmachail Rappresentante degli Studenti x

È presente il Dott. Francesco Paolo D'Elia, Direttore Amministrativo, che assume la funzione di Segretario Verbalizzante.

Il Presidente prosegue a questo punto con lo svolgimento dell'ordine del giorno di cui al citato provvedimento di convocazione, come di seguito riportato:

	Argomento	Relatore	I/P/D/R[1]	note
1	Approvazione verbale seduta precedente	Presidente	D	
2	Adempimento decreto NIS	DA	D	

Si procede pertanto all'esame e alle deliberazioni relative ai punti di cui sopra.

1. Approvazione verbale seduta precedente.

Il Presidente sottopone al Consiglio il verbale in oggetto (n. 8 prot. n. 4608/B1 del 30/9/2026), già in possesso dei consiglieri a seguito dell'invio dello stesso, da parte del DA, nella casella mail dedicata.

Il Consiglio, all'unanimità,

DELIBERA N. 74

di approvare il verbale n. 8 prot. n. 4608/B1 del 30/9/2026.

[1] *Informativa/Proposta/Decisione/Ratifica

2. Adempimento decreto NIS.

Il Presidente introduce il Dott. Agostino Olivieri e la Dott.ssa Claudia Giugni, esponenti della Sicurdata s.r.l., per meglio illustrare l'oggetto della delibera.

Il Dott. Olivieri procede ad una sintetica disamina dei contenuti del D. Lgs. 138/2024 e degli adempimenti di legge a cui l'Istituto è tenuto. Descrive poi sinteticamente quanto già posto in essere sul portale dell'Agenzia di Cybersicurezza Nazionale e, pertanto, il Consiglio prende atto del completamento con successo delle prime fasi obbligatorie previste dalla Direttiva (UE) 2022/2555 e del D.lgs. 138/2024. Si dà atto che ISIA Firenze, in qualità di "Soggetto importante" ai fini NIS2, ha rispettato le seguenti scadenze da rispettare tramite la Piattaforma dell'Agenzia per la Cybersicurezza Nazionale (ACN):

- Registrazione sul Portale, effettuata entro il termine del 28 febbraio 2025;
- Aggiornamento anagrafico definitivo entro il 31 luglio 2025;
- Nomina del Punto di Contatto (PdC), formalizzata contestualmente alla registrazione;
- Designazione del Referente CSIRT, conclusa entro la scadenza perentoria del 31 dicembre 2025;
- invio dell'aggiornamento annuale sul Portale (comprensivo di invio dell'elenco dei fornitori rilevanti)
- invio della Categorizzazione delle attività e dei processi interni di ISIA Firenze che coinvolgono i sistemi informativi.
- Istituzione del Gruppo di lavoro NIS2

Con riguardo all'aggiornamento annuale, si riporta che annualmente, il PdC sarà tenuto a rientrare sulla Piattaforma ed effettuare una verifica complessiva delle informazioni inserite (che da quest'anno includono l'individuazione dei cc.dd. "Fornitori rilevanti") nel periodo 15 aprile - 31 maggio, nonché a comunicare ogni eventuale variazione entro 14 giorni.

Allo stesso modo, la Categorizzazione delle attività dovrà essere confermata o modificata entro il 30 giugno di ogni anno.

Il Consiglio prende atto che la suddetta normativa introduce un principio di responsabilità diretta e personale in capo agli organi direttivi. L'Organo Direttivo è chiamato non solo ad approvare le misure di gestione dei rischi di cybersicurezza, ma anche a sovrintenderne l'attuazione e a partecipare a percorsi di formazione obbligatoria. L'inadempimento di tali obblighi può comportare sanzioni amministrative rilevanti e impatti diretti sulla reputazione e l'operatività aziendale.

Il Consiglio si sottopone, nella propria qualità di organo direttivo, alla sessione formativa avente ad oggetto "Cyber Governance e Responsabilità Straordinaria del CdA ai sensi del Decreto NIS2", della durata complessiva di 1 ora.
La formazione è finalizzata a soddisfare i requisiti dell'art. 23 del D.Lgs. 138/2024 (formazione degli organi direttivi), fornendo ai partecipanti un quadro di sintesi sulle responsabilità strategiche, legali e operative connesse alla disciplina NIS2.
Si dà atto che è stata fornita ai partecipanti la documentazione di sintesi / slide della presentazione, già allegati alla relazione accompagnatoria al provvedimento di convocazione dell'odierna seduta e che sarà svolta anche una sessione specifica per i consiglieri che non dispongono di deleghe di poteri.
L'articolazione dei contenuti della formazione è di seguito specificata come da tabella.

Durata	**Modulo**	**Contenuti**	**Obiettivo**
Modulo 1 – 00:00 / 07:00	Il quadro normativo NIS2 e il ruolo di ACN	Perché il soggetto rientra nel perimetro NIS2; ruolo dell'Agenzia per la Cybersicurezza Nazionale; recente comunicazione PEC inviata dall'Autorità.	Comprendere il contesto legale e istituzionale.
Modulo 2 – 07:00 / 15:00	Responsabilità, Governance e Articolo 23	Ruolo dei membri del CdA senza deleghe operative; responsabilità dell'Organo di Amministrazione sull'approvazione del piano di mitigazione dei rischi; dovere di vigilanza.	Chiarire il confine tra gestione operativa e responsabilità di supervisione statutaria.

Modulo 3 – 15:00 / 22:00	Le scadenze operative e la gestione degli incidenti	Stato degli adempimenti: notifica incidenti CSIRT Italia già attiva e traguardo Misure di Sicurezza di Base a ottobre 2026; processo di gestione delle crisi da parte del CdA; presentazione del sistema "SIGN2 – Sistema di Gestione Integrato NIS2" implementato.	Comprendere scadenze, processi di gestione degli incidenti e strumenti organizzativi.
Modulo 4 – 22:00 / 30:00	Q&A e Discussione	Sessione aperta per chiarire dubbi dei Consiglieri circa l'impatto delle misure sui processi decisionali e sulla conformità dell'ente.	Favorire il confronto e verificare la comprensione dei principali temi trattati.

Il Consiglio prende poi atto che ISIA Firenze ha implementato il progetto SIGN2 - Sistema di Gestione NIS2. Tale sistema è concepito per integrare i controlli di sicurezza informatica previsti dalla normativa NIS2 con gli adempimenti in materia di protezione dei dati personali previsti dal GDPR e armonizzare la documentazione del Sistema di Gestione Sicurezza Informatica.
Gli aspetti chiave del progetto sono i seguenti:

- Predisposizione e formalizzazione di politiche di sicurezza, procedure operative, standard di controllo, registri e modelli documentali.
- Allineamento con i requisiti tecnici e organizzativi previsti per i soggetti NIS2.
- Coinvolgimento delle funzioni aziendali di Governance, Risk & Compliance, Sicurezza ICT e Amministrazione.
- Termine previsto per il completamento del Sistema: ottobre 2026, in conformità ai termini stabiliti dalla Determina ACN 164179/2025 per i soggetti importanti.

Al fine di ottemperare a questi obblighi, il Consiglio prende atto che ISIA Firenze ha implementato le misure di sicurezza di base richieste dalla normativa e dall'Autorità di Cybersicurezza Nazionale. L'elenco dei documenti e delle attività che richiedono l'approvazione dell'Organo Direttivo viene allegato al presente verbale.
Tra gli obblighi già in vigore rientra quello di implementare e redigere un Incident Response Plan (IRP), ossia un piano di risposta agli incidenti di sicurezza informatica, come requisito obbligatorio ai fini della gestione degli incidenti e della notifica al CSIRT Italia (art. 25 decreto NIS).
Il suddetto documento, unitamente ad altri documenti aggiuntivi completi, viene sottoposto all'attenzione del Consiglio e a tal fine si dà atto che i seguenti documenti sono stati sottoposti all'attenzione e alla deliberazione del Consiglio. Gli stessi, tramite il link di riferimento, sono da ritenersi parte integrante del presente verbale ove indicato essere da approvare:

#	Documento ACN (CdA)	Riferimento Requisito	Riscontro nel GANTT ISIA	Stato dell'Arte / Note operative ISIA
1	Organizzazione per la sicurezza informatica	GV.RR-02 (punto 1)	Riga 7 & 8: Organigramma e Elenco Personale con Ruoli/Responsabilità	COMPLETATO. Approvato dal CdA come da Verbale n. 4 del 25/06/2026.
2	Politiche di sicurezza informatica: 1. Per il controllo degli accessi 2. Di cifratura e sicurezza dei dati 3. Procedura di esecuzione e test di backup	GV.PO-01 (punto 3)	Riga 26: Politica di sicurezza dei sistemi informativi e di rete (con richiamo alle politiche specifiche)	IN CORSO / BOZZA. Le singole politiche d'ambito (Accessi, Backup, Cifratura, Supply Chain) sono in fase di revisione/verifica con Bonomi, Mari e il fornitore N3tcom.
3	Valutazione del rischio posto alla sicurezza dei sistemi	ID.RA-05 (punto 3)	Riga 18: Valutazione del rischio (identificazione,	IN CORSO. In data 05/08 è stato caricato il *template*

#	Documento ACN (CdA)	Riferimento Requisito	Riscontro nel GANTT ISIA	Stato dell'Arte / Note operative ISIA
	informativi e di rete		analisi e ponderazione)	nella cartella 6 del SIGN.
4	Piano di trattamento del rischio	ID.RA-06 (punto 3)	Riga 20: Politica di gestione del rischio / Piano di gestione del rischio (opzioni di trattamento e mitigazione)	IN CORSO. Documentazione legata alla gestione e al trattamento del rischio inserita tra le attività in lavorazione nel piano.
5	Piano di gestione delle vulnerabilità	ID.RA-08 (punto 4)	Riga 20: Piano di gestione delle vulnerabilità	IN CORSO. Previsto all'interno della macro-attività sulla gestione del rischio e gestione vulnerabilità.
6	Piano di adeguamento	ID.IM-01 (punto 1)	Riga 35: Piano di adeguamento (in accordo con gli esiti del Riesame della Direzione)	IN CORSO / IN PROGRAMMAZIONE. Collegato al riesame della Direzione ex GV.PO-02.
7	Piano di continuità operativa	ID.IM-04 (punto 4)	Riga 11: Procedura di Business Continuity & Disaster Recovery	IN CORSO. SDT ha caricato il nuovo template integrato con info N3tcom (cartella 7 SIGN); verifica del documento in corso (Bonomi/Mari).

#	Documento ACN (CdA)	Riferimento Requisito	Riscontro nel GANTT ISIA	Stato dell'Arte / Note operative ISIA
8	Piano di ripristino in caso di disastro	ID.IM-04 (punto 4)	Riga 11: Procedura di Business Continuity & Disaster Recovery	IN CORSO. Gestito congiuntamente al Piano di Continuità Operativa nella cartella 7 del SIGN.
9	Piano di gestione delle crisi	ID.IM-04 (punto 4)	Riga 4 & 11: Incident Response Plan / BC&DR	IN CORSO. Integrato negli schemi di Business Continuity e Incident Response gestiti con i fornitori/consulenti.
10	Piano di formazione	PR.AT-01 (punto 2)	Riga 21: Piano di formazione (approvazione CdA)	IN CORSO. Mappato a GANTT come documento destinato all'approvazione del CdA.
11	Piano per la gestione degli incidenti di sicurezza informatica	RS.MA-01 (punto 2)	Riga 4: Incident Response Plan (approvazione CdA)	IN CORSO. Documento integrato con contributi del fornitore; in fase di verifica finale da parte di Bonomi e Mari.

Pertanto, il Consiglio, all'unanimità,

VISTA la legge 21 dicembre 1999, n. 508, di riforma delle Accademie di Belle Arti, dell'Accademia Nazionale di Danza, dell'Accademia Nazionale di Arte Drammatica, degli Istituti Superiori per le Industrie Artistiche, dei Conservatori di Musica e degli Istituti Musicali Pareggiati;

VISTO il D.P.R. 28 febbraio 2003, n. 132, recante i criteri per l'autonomia statutaria, regolamentare e organizzativa delle suddette istituzioni;

VISTO lo Statuto dell'Istituto superiore per le Industrie Artistiche (ISIA) di Firenze, approvato con D.D. n. 97 del 4/2/2025;

VISTO il D. Lgs. 138/2024;

VISTA la determinazione ACN n. 379887 del 19/12/2025;

PRESO ATTO della relazione del Dott. Agostino Oliveri e della Dott.ssa Claudia Giugni nell'odierna seduta ed esaminata la documentazione sottoposta,

DELIBERA N. 75

di approvare i documenti indicati nelle premesse e nella conseguente tabella, ove indicato nelle premesse medesime, ai fini degli adempimenti previsti dal D. Lgs. 138/2024 in materia di cybersicurezza.

Non essendovi altre questioni da discutere o da sottoporre all'attenzione del Consiglio, il Presidente dichiara conclusi i lavori e lo scioglimento della seduta alle ore 16.40.

Letto, approvato e sottoscritto.

Il SEGRETARIO VERBALIZZANTE

Dott. Francesco Paolo D'Elia

D'ELIA
FRANCESCO
PAOLO
06.11.2026
14:19:01
GMT+01:00

IL PRESIDENTE

Arch. Massimiliano Morlacci

Morlacci
Massimiliano
06.11.2026
13:07:48
UTC