REGOLAMENTO PER L'USO DEI SISTEMI INFORMATIVI E DELL'INTELLIGENZA ARTIFICIALE

Ordine degli Ingegneri di Ferrara - Revisione 1.01 Dicembre 2025

Approvato con Verbale n. 20 del 02.12.2025

INDICE RAPIDO

1. Scopo, oggetto e perché serve
2. Ambito e destinatari
3. Definizioni chiave
4. Governance e ruoli (chi fa cosa)
5. Classificazione dei dati e regole di accesso
6. Identità digitali, password, MFA e credenziali tecniche
7. Dispositivi, BYOD e supporti rimovibili
8. Email, web, messaggistica e social
9. Software, licenze, installazioni e assistenza remota
10. Rete, accesso da remoto e Wi-Fi
11. Backup, archiviazione, conservazione e distruzione sicura
12. Logging, monitoraggio e tutela dei lavoratori
13. Incidenti e vulnerabilità: come segnalarli e gestirli
14. Continuità operativa e disaster recovery (DR)
15. Uso dei tool di Intelligenza Artificiale (IA) – principi, divieti, casi d'uso
16. IA nei procedimenti amministrativi (trasparenza e tracciabilità)
17. IA e risorse umane (selezione, turni, valutazioni)
18. Appalti e fornitori (clausole minime IA/ICT)
19. Formazione, consapevolezza e verifica periodica
20. Sanzioni interne e responsabilità
21. Entrata in vigore, revisione e piano di transizione

Allegati:

A) Scheda di Trasparenza IA •

B) Registro Uso IA •

C) Clausole contrattuali minime •

D) FRIA/DPIA – checklist e matrice rischi •

E) Procedura Incident (con moduli) •

F) Policy Password e Credenziali •

G) Moduli operativi (presa visione, BYOD, richiesta utenza) •

H) Modello “Nota di motivazione con IA” •

I) Etichettatura contenuti sintetici •

J) Informativa HR sistemi automatizzati •

K) Piano di audit annuale.

---

1. Scopo, oggetto e perché serve

Questo regolamento stabilisce regole chiare per l’uso sicuro e conforme dei sistemi informatici dei servizi di intelligenza artificiale (IA), con l’obiettivo di tutelare utenti e dipendenti dell’organizzazione. Serve a ridurre i rischi di violazioni dei dati, errori, interruzioni di servizio e contenziosi, garantendo trasparenza nell’uso degli algoritmi e delle tecnologie digitali.

2. Ambito e destinatari

Il regolamento si applica a:

- Dipendenti, dirigenti, amministratori, collaboratori, tirocinanti, fornitori e chiunque tratti dati o utilizzi servizi ICT/IA per conto dell’Ordine, sia in sede che da remoto.
- Tutti coloro che, a qualsiasi titolo, accedono ai sistemi informativi o trattano dati dell’Organizzazione.

3. Definizioni chiave

- **Sistema informativo:** Insieme di persone, processi, applicazioni e infrastrutture che gestiscono dati e servizi digitali.
- **Sistema di IA:** Software che genera output (testi, immagini, raccomandazioni, punteggi) utilizzati per decisioni o supporto decisionale.
- **Alto rischio (IA):** Usi dell'IA che incidono su diritti fondamentali (es. graduatorie, benefici sociali, gestione lavoratori) e richiedono controlli aggiuntivi.
- **Controllo umano significativo:** Una persona può comprendere, correggere e bloccare l'algoritmo, garantendo la supervisione sulle decisioni

4. Governance e ruoli

- **Il Consiglio dell'ordine** approva il Regolamento
- **Consigliere Segretario** vigila sulla conformità amministrativa e procedurale
- **DPO (Responsabile Protezione Dati):** Garantisce la privacy by design, fornisce pareri su DPIA/FRIA e valuta i data breach.
- **RPCT:** Assicura coerenza con le politiche di anticorruzione e trasparenza.
- **CED/IT:** Cura la sicurezza IT, il backup, la gestione degli accessi, la VPN, il MDM ove esistente e la gestione degli incidenti.
- **Personale:** Rispetta le regole e segnala incidenti e vulnerabilità entro 24 ore.
- **Fornitori:** Devono rispettare le clausole contrattuali e collaborare ad audit, log, explainability e gestione degli incidenti.

5. Classificazione dei dati e regole di accesso

- I dati sono classificati come: pubblici, interni, riservati, personali, particolari (es. salute) o giustizia/sicurezza.
- L'accesso ai dati è consentito solo ai ruoli autorizzati, secondo il principio del minimo privilegio. Gli account condivisi sono vietati.
- In caso di emergenza ("break-glass"), l'accesso può essere concesso solo con approvazione del Responsabile di Servizio e tracciatura.
- I fornitori hanno accesso solo temporaneo, profilato e loggato, con obbligo di NDA e chiusura degli accessi a fine attività.
- Gli utenti devono chiedere solo gli accessi necessari e segnalare eventuali permessi eccessivi o dati non pertinenti al CED

6. Identità digitali, password, MFA e credenziali tecniche

- Gli account devono essere nominativi e le credenziali non possono essere cedute.
- **Password**: minimo 12 caratteri con complessità; Vietato il riuso su sistemi critici; Necessario il cambio immediato al sospetto di compromissione; Si vieta il “salvataggio in chiaro” delle password all’interno di file di testo dal nome “ Password” o “Credenziali”.
- **MFA** (doppio livello di autenticazione) obbligatoria per posta, VPN, gestionali, cloud, console amministrative.
- **Admin e privilegiati**: Le utenze vanno separate dalle ordinarie secondo gruppi; Il limite per le sessioni temporale deve essere il minimo possibile; Si richiede auditing rafforzato.
- **API keys/token/service account**: Il rilascio avviene dal CED o dal servizio informatico in outsourcing applicando i principi di: ambito minimo, rotazione, custodia in **vault**; inventario e scadenze vanno entrambi documentati.

7. Dispositivi, BYOD e supporti rimovibili

- **Cifratura disco**: Tutti i computer e notebook forniti devono avere il disco rigido cifrato. Questo significa che i dati memorizzati sono protetti da una codifica che li rende illeggibili a chi non possiede le credenziali di accesso. Serve a prevenire la perdita o il furto di dati in caso di smarrimento o furto del dispositivo.
- **EDR/antivirus**: È obbligatorio installare sistemi di sicurezza come EDR (Endpoint Detection and Response) e antivirus. Questi strumenti monitorano costantemente il computer per rilevare, bloccare e rispondere a minacce informatiche come virus, malware o attacchi sospetti.
- **Patch**: I dispositivi devono essere sempre aggiornati con le ultime patch di sicurezza. Le patch sono aggiornamenti rilasciati dai produttori per correggere vulnerabilità o errori che potrebbero essere sfruttati da malintenzionati.

- **Screen-lock ≤30’**: Deve essere attivato il blocco automatico dello schermo dopo un massimo di 10 minuti di inattività. Questo riduce il rischio che persone non autorizzate possano accedere ai dati se il dispositivo viene lasciato incustodito.
- **BYOD** significa "Bring Your Own Device", cioè l’uso di dispositivi personali (come smartphone, tablet o computer portatili) per accedere ai dati o ai sistemi dell’organizzazione.
  Puoi usare il tuo smartphone o PC personale per lavorare con dati o sistemi solo se hai un’autorizzazione formale e il dispositivo è protetto da sistemi di sicurezza gestiti. In assenza di queste condizioni, è vietato usare dispositivi personali per attività lavorative che coinvolgono dati dell’Organizzazione.

- **Uso limitato delle USB**: Le chiavette USB e altri dispositivi di memoria esterna possono essere utilizzati solo quando è strettamente necessario per motivi di lavoro. Non è permesso usarli liberamente o per comodità personale.

- **Solo supporti cifrati e approvati**: Si possono utilizzare solo dispositivi USB che sono stati cifrati (cioè protetti da una codifica che rende i dati leggibili solo a chi ha le credenziali) e che sono stati approvati. Questo serve a proteggere i dati da furti o smarrimenti.
- **Niente copie inutili**: Non è permesso fare copie di dati su USB se non strettamente necessario. L'obiettivo è ridurre il rischio di dispersione o perdita di informazioni sensibili.

  In sintesi:
  L'uso delle chiavette USB è fortemente regolamentato: puoi usarle solo se sono cifrate e autorizzate, e solo per operazioni davvero necessarie. Non si devono fare copie di dati che non servono, per evitare rischi di sicurezza

8. E-mail, web, messaggistica e social

E-mail solo per fini istituzionali; allegati sensibili con cifratura/PEC ove richiesto

Le email devono essere utilizzate esclusivamente per attività lavorative e comunicazioni ufficiali. Se devi inviare allegati che contengono dati critici (ad esempio dati personali, informazioni riservate), questi devono essere protetti tramite cifratura (cioè resi leggibili solo ai destinatari autorizzati tramite, ad esempio, zip con password) oppure inviati tramite PEC (Posta Elettronica Certificata), che garantisce sicurezza e tracciabilità.

Esempio pratico:

- Se devi inviare un documento con dati personali di utenti, devi cifrarlo o usare la PEC.
- Non usare la mail lavorativa per scopi personali.

Attenzione a phishing e link sospetti; usa il canale "segnala phishing"

Bisogna prestare molta attenzione a e-mail sospette che potrebbero contenere tentativi di phishing (cioè truffe informatiche che cercano di rubare dati o credenziali). Se ricevi un'e-mail con link strani o richieste insolite, non cliccare e segnala subito l'episodio tramite il canale ufficiale "segnala phishing". E' inoltre proibita la navigazione su siti non rispondenti alle esigenze professionali dell'organizzazione.

Esempio pratico:

- Ricevi una mail che ti chiede di inserire la password su un sito sconosciuto? Non cliccare e segnala subito l'e-mail al reparto IT tramite la funzione di outlook "Segnala posta indesiderata"

Chat (Teams/altro): bene per coordinamento operativo; non inviare dati particolari a canali non protetti

Le chat interne (come Teams) sono utili per coordinarsi rapidamente tra colleghi. Tuttavia, non bisogna mai inviare dati sensibili o particolari (ad esempio dati sanitari, giudiziari, ecc.) su canali che non sono protetti o autorizzati.

Esempio pratico:

- Puoi usare Teams per organizzare una riunione o condividere informazioni operative.
- Non inviare tramite chat documenti con dati personali o informazioni riservate, a meno che il canale sia protetto e autorizzato.

Social: pubblicano solo gli incaricati; contenuti sintetici (IA) etichettati (vedi Allegato I)

L'uso di social personali su strumenti aziendali è proibito.
Solo le persone autorizzate dall'organizzazione possono pubblicare contenuti sui social network ufficiali, ove esistenti. Se vengono pubblicati contenuti generati o modificati con l'Intelligenza Artificiale (IA), questi devono essere chiaramente etichettati come tali, secondo quanto previsto dall'Allegato I del regolamento.

9. Software, licenze, installazioni e assistenza remota

Installazioni solo da catalogo approvato o previa richiesta

Si possono installare programmi e applicazioni solo se fanno parte di un elenco ufficiale (catalogo approvato) predisposto dall'Organizzazione, oppure se si è fatta una richiesta formale e questa è stata autorizzata.

Esempio pratico:

- Se hai bisogno di un nuovo software per lavorare, prima controlla se è già nel catalogo approvato.

- Se non lo è, devi chiedere l'autorizzazione all'ufficio IT o al responsabile, che valuterà la richiesta.

Vietato software non licenziato; aggiornamenti di sicurezza tempestivi

È vietato installare o utilizzare software senza regolare licenza (cioè pirata o scaricato illegalmente). Tutti i programmi devono essere aggiornati tempestivamente con le ultime patch di sicurezza, per ridurre i rischi di vulnerabilità.

Esempio pratico:

- Non puoi installare versioni gratuite o "crackate" di programmi a pagamento.
- Quando ricevi una notifica di aggiornamento di sicurezza per un software, devi eseguirlo il prima possibile.

Teleassistenza: su richiesta, con consenso e logging delle operazioni

L'assistenza remota (cioè quando un tecnico accede al tuo computer a distanza) può essere attivata solo se la richiedi tu o il responsabile, e solo dopo aver dato il consenso. Tutte le operazioni svolte durante la teleassistenza devono essere registrate (logging), per garantire trasparenza e sicurezza.

Esempio pratico:

- Se hai un problema tecnico, puoi chiedere la teleassistenza. Prima che il tecnico si colleghi, devi dare il tuo consenso.
- Tutte le azioni fatte dal tecnico saranno tracciate e registrate, così da poterle verificare in caso di necessità.

10. Rete, accesso da remoto e Wi-Fi

Accesso remoto solo tramite VPN con MFA

Per collegarsi ai sistemi informatici dell'Organizzazione da fuori sede (ad esempio da casa o da una postazione esterna), è obbligatorio utilizzare una VPN (Virtual Private Network) e l'autenticazione a più fattori (MFA, valida anche tramite password+certificato).

- **VPN**: crea un “tunnel” sicuro tra il dispositivo dell’utente e la rete dell’organizzazione, proteggendo i dati trasmessi da intercettazioni o attacchi.
- **MFA**: richiede almeno due metodi di verifica (ad esempio password + codice temporaneo sul telefono), aumentando la sicurezza contro accessi non autorizzati.

Esempio pratico:
Se lavori da remoto, devi prima attivare la VPN e poi autenticarti con MFA per accedere ai sistemi comunali.

Wi-Fi ospiti separato; reti interne segmentate; firewall e IDS/IPS gestiti dal CED

- **Wi-Fi ospiti separato**: la rete Wi-Fi per i visitatori deve essere distinta e isolata da quella interna, per evitare che chi si collega come ospite possa accedere a dati o sistemi riservati.
- **Reti interne segmentate**: la rete informatica interna è suddivisa in “segmenti” separati (ad esempio uffici diversi o servizi diversi), così da limitare i danni in caso di incidente o attacco.
- **Firewall e IDS/IPS gestiti dal CED**: il Centro Elaborazione Dati (CED) si occupa di configurare e gestire firewall (barriere di sicurezza) e sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS), per monitorare e bloccare attività sospette.

Esempio pratico:
Un visitatore può navigare su Internet tramite la rete ospiti, ma non può accedere ai documenti interni. Se un attacco informatico colpisce un ufficio, la segmentazione limita la propagazione ad altri uffici.

---

3. Vietato l’uso di Wi-Fi pubblici non protetti senza VPN

Non è permesso collegarsi ai sistemi usando reti Wi-Fi pubbliche (ad esempio in bar, aeroporti, hotel) se non si utilizza la VPN. Le reti pubbliche sono spesso poco sicure e possono essere facilmente intercettate da malintenzionati.

Esempio pratico:
Se sei fuori ufficio e vuoi accedere a dati o servizi dell’Organizzazione, puoi farlo solo se prima attivi la VPN; altrimenti, l’accesso è vietato.

11. Backup, archiviazione, conservazione e distruzione sicura

Backup secondo piano IT; test di ripristino periodici

I dati e i sistemi informatici dell'Organizzazione vengono sottoposti a backup (copie di sicurezza) seguendo un piano IT definito. Questo piano stabilisce cosa, quando e come deve essere salvato per garantire che, in caso di problemi (guasti, attacchi informatici, errori umani), sia possibile recuperare le informazioni.
Inoltre, vengono effettuati test periodici di ripristino: si prova concretamente a recuperare i dati dai backup per assicurarsi che il sistema funzioni davvero e che i dati siano effettivamente recuperabili.

---

2. Conservazione secondo il piano di conservazione; versioning ove possibile

I dati vengono conservati per il tempo previsto dal piano di conservazione, che stabilisce per quanto tempo ogni tipo di documento o informazione deve essere mantenuto.

Dove possibile, si applica il versioning, cioè la conservazione di più versioni di uno stesso documento, così da poter recuperare versioni precedenti in caso di errori o modifiche non volute.

Esempio pratico:
Un documento protocollato viene conservato per 10 anni come previsto dalla normativa. Se viene modificato più volte, il sistema tiene traccia delle varie versioni, così da poter tornare a una versione precedente se necessario.

---

3. Distruzione sicura: cancellazione certificata/shredding per supporti e carta

Quando i dati non sono più necessari o scade il periodo di conservazione, devono essere eliminati in modo sicuro.

- Per i dati digitali, si usa la cancellazione certificata: i file vengono eliminati in modo che non possano essere recuperati.
- Per i supporti fisici (hard disk, chiavette USB) e la carta, si utilizza lo shredding, cioè la distruzione fisica tramite triturazione.

12. Logging, monitoraggio e tutela dei lavoratori

Il CED registra log tecnici di accessi e operazioni rilevanti per sicurezza/continuità

Il Centro Elaborazione Dati (CED) tiene traccia, attraverso dei "log tecnici", di tutte le attività importanti che avvengono sui sistemi informatici. Questi log includono, ad esempio, chi accede ai sistemi, quali operazioni vengono svolte e quando.
Lo scopo è duplice:

- **Sicurezza:** Permettere di individuare eventuali accessi non autorizzati, tentativi di attacco o comportamenti anomali.
- **Continuità operativa:** Avere una traccia delle attività per poter ricostruire cosa è successo in caso di problemi tecnici o incidenti.

Niente controlli occulti: ogni monitoraggio è proporzionato, documentato e comunicato ai dipendenti tramite informativa

Il regolamento vieta qualsiasi forma di controllo nascosto o non dichiarato sui lavoratori.

- **Monitoraggio proporzionato:** Il controllo deve essere limitato a quanto strettamente necessario per garantire la sicurezza e la continuità dei servizi, senza invadere la privacy dei dipendenti.
- **Documentato:** Tutte le attività di monitoraggio devono essere registrate e tracciabili.
- **Comunicazione tramite informativa:** I dipendenti devono essere informati in modo chiaro e trasparente su quali controlli vengono effettuati, perché e come vengono gestiti i dati raccolti.

13. Incidenti e vulnerabilità: come segnalarli e gestirli

Segnalazione tempestiva degli incidenti:
L'utente deve segnalare entro 24 ore qualsiasi evento che possa compromettere la sicurezza o la disponibilità dei sistemi informatici. Questo include:

- infezioni da malware (software dannoso),
- furto o smarrimento di dispositivi (come computer o smartphone),
- invio errato di dati a destinatari non autorizzati,
- sospetti di violazione dei dati (data breach),
- compromissione delle credenziali di accesso (ad esempio password rubate),

- risultati prodotti dall'Intelligenza Artificiale che siano gravemente errati o discriminatori,
- indisponibilità dei servizi informatici (es. sistemi bloccati o non funzionanti).

Gestione dell'incidente:
Il Centro Elaborazione Dati (CED) si occupa di coordinare tutte le attività necessarie per contenere il problema e ripristinare il corretto funzionamento dei sistemi. Il Responsabile della Protezione dei Dati (DPO) ove incaricato valuta se sia necessario notificare l'incidente al Garante per la privacy o ai cittadini coinvolti, in base alla gravità e alla natura dell'evento.

Procedura e modulistica:
Per segnalare correttamente un incidente, vanno utilizzati i moduli specifici previsti nell'Allegato E del regolamento, che guidano nella raccolta delle informazioni essenziali per la gestione e la risoluzione dell'evento.

14. Continuità operativa e disaster recovery (DR)

Sistemi critici con RTO/RPO dichiarati; prove periodiche di failover/restore

Spiegazione:
I sistemi informatici considerati "critici" (cioè fondamentali per il funzionamento dell'Organizzazione) devono avere chiaramente definiti due parametri:

- **RTO (Recovery Time Objective):** il tempo massimo accettabile per il ripristino del servizio dopo un'interruzione.
- **RPO (Recovery Point Objective):** la quantità massima di dati che si può perdere, espressa come intervallo di tempo (ad esempio, massimo 1 ora di dati persi).

Inoltre, devono essere effettuate regolarmente delle prove pratiche di **failover** (passaggio automatico a un sistema di backup in caso di guasto) e di **restore** (ripristino dei dati e dei servizi da backup), per assicurarsi che i sistemi siano davvero recuperabili in caso di emergenza.

---

2. Piano di subentro manuale per servizi essenziali (es. protocollazione di emergenza)

Spiegazione:
Per i servizi essenziali (quelli che non possono essere interrotti, come la protocollazione), deve essere predisposto un **piano di subentro manuale**.
Questo significa che, se i sistemi informatici non sono disponibili, il personale deve sapere come continuare a svolgere le attività fondamentali in modalità manuale (ad esempio, registrando i protocolli su carta), fino al ripristino dei sistemi digitali.

15. Uso dei tool di Intelligenza Artificiale (IA) – principi, divieti, casi d'uso

Principi fondamentali:
L'utilizzo di strumenti di IA deve sempre rispettare i seguenti principi:

- **Trasparenza:** è necessario informare chiaramente quando e come viene utilizzata l'IA, sia verso i clienti che all'interno dell'Organizzazione.
- **Tracciabilità:** tutte le operazioni svolte con l'IA devono essere registrate e documentate, in modo da poter ricostruire le attività effettuate.
- **Controllo umano:** ogni decisione automatizzata deve essere supervisionata da una persona che abbia la possibilità di comprendere, correggere o bloccare l'algoritmo.
- **Non discriminazione:** l'IA non deve mai essere utilizzata in modo da creare discriminazioni tra persone o gruppi.
- **Sicurezza lungo il ciclo di vita:** i sistemi di IA devono essere protetti da rischi e vulnerabilità per tutta la loro durata di utilizzo.

Divieti specifici:
Non è consentito utilizzare l'IA per:

- Sistemi di "social scoring" (valutazione delle persone su base sociale).
- Manipolazione subliminale degli utenti.
- Riconoscimento delle emozioni in ambito lavorativo o scolastico.
- Sistemi biometrici non previsti dalla normativa.
- Pubblicazione di contenuti generati dall'IA senza una chiara etichetta che ne indichi l'origine.

Dati da NON inserire in strumenti generativi esterni (come chatbot o generatori di testo/immagini) senza una base giuridica o autorizzazione specifica:

- Dati particolari (ex GDPR ad esempio dati sanitari, religiosi, politici).
- Segreti d'ufficio.
- Contratti non pubblici.
- Credenziali di accesso o configurazioni tecniche.

Casi consentiti, ma solo con revisione umana obbligatoria:

- Bozze di documenti che non contengano nomi di persone.
- FAQ generiche.

- Semplificazioni linguistiche di testi pubblici.
- Traduzioni interne.
- Analisi preliminari di atti pubblici.

Obblighi per i fornitori di IA:
Nei contratti con fornitori di soluzioni IA devono essere inserite clausole che garantiscano:

- La conformità alle normative vigenti.
- La spiegabilità (explainability) delle decisioni dell'IA.
- La registrazione dei log delle attività.
- La gestione degli incidenti.
- Il divieto di utilizzare i dati dell'Organizzazione per addestrare sistemi IA, salvo accordo scritto specifico.

16. IA nei procedimenti (trasparenza e tracciabilità)

Quando un ufficio utilizza sistemi di intelligenza artificiale (IA) all'interno di un procedimento amministrativo, devono essere rispettate le seguenti regole:

- **Scheda di Trasparenza IA:**
  È obbligatorio compilare e pubblicare una "Scheda di Trasparenza IA" (Allegato A) per ogni procedimento o servizio in cui viene impiegata l'IA. Questa scheda serve a informare i cittadini e a documentare in modo chiaro l'uso dell'IA, specificando il sistema utilizzato, le finalità, i dati trattati, le modalità di controllo umano e la base giuridica.
- **Registrazione nel fascicolo:**
  L'uso dell'IA deve essere registrato nel fascicolo del procedimento, indicando quando e perché è stata utilizzata.
- **Nota di motivazione nell'atto finale:**
  L'atto amministrativo conclusivo deve contenere una nota che spiega il contributo fornito dall'IA e il ruolo del controllo umano nella decisione (secondo il modello di Allegato H).

17. IA e risorse umane (selezione, turni, valutazioni)

Prima di utilizzare sistemi di IA per attività relative alle risorse umane (ad esempio selezione del personale, pianificazione dei turni, valutazioni), è necessario:

- **Informativa ai candidati e dipendenti:**
  Fornire un'informativa chiara su scopi, logiche di funzionamento, dati utilizzati, accuratezza, robustezza, sicurezza dei sistemi automatizzati e canali per eventuali contestazioni (secondo il modello di Allegato J).
- **Aggiornamento del registro dei trattamenti:**
  Aggiornare il registro dei trattamenti dei dati personali per includere l'uso di IA in ambito HR.
- **Valutazione DPIA/FRIA:**
  Valutare la necessità di effettuare una DPIA (Valutazione d'Impatto sulla Protezione dei Dati) o una FRIA (Valutazione d'Impatto sui Diritti Fondamentali), soprattutto se vengono trattati dati particolari o se l'uso dell'IA può incidere sui diritti delle persone.
- **Divieto di controlli occulti:**
  È vietato utilizzare l'IA per effettuare controlli nascosti o non dichiarati sui lavoratori.

18. Appalti e fornitori (clausole minime IA/ICT)

Nei capitolati e nei contratti con fornitori di soluzioni ICT e IA devono essere inseriti requisiti minimi che garantiscano la tutela dell'Organizzazione. In particolare:

- **Conformità normativa:** Il fornitore deve dichiarare la conformità alle normative europee e italiane in materia di intelligenza artificiale, privacy e amministrazione digitale. Per gli usi ad alto rischio, devono essere fornite evidenze di valutazione di conformità, manuali e istruzioni d'uso.
- **Trasparenza tecnica:** Il fornitore deve descrivere chiaramente le funzioni, i limiti e le metriche di accuratezza e robustezza dei sistemi, garantendo una spiegabilità adeguata all'uso previsto.
- **Dati e sicurezza:** Devono essere garantiti la crittografia dei dati, la gestione delle vulnerabilità, il rafforzamento della sicurezza (hardening), i test di sicurezza, la business continuity e il disaster recovery (BCDR), la localizzazione dei dati nell'Unione Europea e la notifica degli incidenti entro 24 ore.
- **Log ed export:** Deve essere prevista la possibilità di esportare log e tracciati pertinenti, nonché la cooperazione a valutazioni di impatto sui diritti fondamentali (FRIA/DPIA) e audit.
- **Subfornitura:** È ammessa solo previa autorizzazione, con elenco e responsabilità su eventuali sub-processori.

- **Diritti e proprietà intellettuale:** Devono essere chiariti i diritti di licenza e d'uso degli output, la consegna dei materiali in caso di recesso (escrow) e la portabilità dei dati.
- **Contenuti sintetici:** Deve essere previsto il watermark o l'etichettatura dei contenuti generati da IA, e il divieto di utilizzare i dati dell'Organizzazione per addestrare sistemi IA, salvo accordo scritto.
- **SLA e penali:** Devono essere definiti tempi di presa in carico e ripristino, nonché penali per disservizi e non conformità.

19. Formazione, consapevolezza e verifica periodica

- **Formazione:** Tutto il personale deve partecipare annualmente a brevi moduli di formazione su phishing, gestione delle password, trattamento dei dati, uso sicuro dell'IA, prevenzione dei bias e controllo umano, e segnalazione degli incidenti.
- **Verifica periodica:** Periodicamente devono essere verificati accessi, log, backup, schede di trasparenza IA e clausole contrattuali.
  Queste attività servono a mantenere alto il livello di consapevolezza e a garantire il rispetto delle regole di sicurezza e trasparenza.

20. Sanzioni interne e responsabilità

- **Responsabilità:** Chi viola le regole del presente regolamento è soggetto a responsabilità disciplinare, civile, contabile e penale, secondo le norme e i codici interni dell'Organizzazione.
- **Sanzioni:** Le sanzioni possono essere applicate in caso di comportamenti non conformi, omissioni, negligenze o azioni che mettano a rischio la sicurezza, la privacy o la continuità operativa dei sistemi informativi.

21. Entrata in vigore, revisione e piano di transizione

- **Entrata in vigore**: Il regolamento entra in vigore in data 02.12.2025 con Delibera n.ro 2 /verb. 20 /2025.
- **Revisione:** Il regolamento viene rivisto almeno una volta all'anno, oppure in caso di cambiamenti normativi o organizzativi rilevanti.

- **Piano di transizione:** Nei 120 giorni successivi all’adozione, devono essere completate le seguenti attività:
    - Attivazione dell’autenticazione a più fattori (MFA) su tutti i sistemi critici.
    - Pubblicazione delle schede di trasparenza IA.
    - Aggiornamento delle informative HR.
    - Attivazione dei moduli per la segnalazione degli incidenti.
    - Inserimento delle clausole IA nei nuovi affidamenti e contratti.