

P1.1-3

Informativa clienti per l'utilizzo di servizi Cloud

(UNI EN ISO 9001:2015 - UNI CEI EN ISO/IEC 27001:2024 –
UNI CEI EN ISO/IEC 27017:2021)

Ver.2	24/06/2025	2° Rilascio	MB	Management Team	CEO	PUBBLICO
REVISIONE	DATA	MODIFICA	REDATTO	VERIFICATO	APPROVATO	RISERVATEZZA

Camillo Ghelfi, CEO 40Factory



Sommario

INTRODUZIONE	4
AMBITO DI APPLICAZIONE	4
PRINCIPI DI CONFORMITÀ	4
STRUTTURA DI SICUREZZA DEI SERVIZI BASATA SU RUOLI E RESPONSABILITÀ	5
MODELLO DI RESPONSABILITÀ CONDIVISA	5
<i>Tabella responsabilità MAT CLOUD (SaaS)</i>	6
<i>Tabella responsabilità Mat Control center (MCC)</i>	7
<i>Tabella responsabilità WILSON Cloud (SaaS)</i>	8
RUOLI E RESPONSABILITÀ	9
MISURE TECNICHE ED ORGANIZZATIVE PER LA SICUREZZA	10
FORMAZIONE DEI DIPENDENTI	10
REGOLAMENTO AZIENDALE E CODICE ETICO	10
POLITICA DEI PRIVILEGI MINIMI - USER MINIMUM PRIVILEGE	11
REGOLE PER LA GESTIONE DEGLI ACCESSI	11
GESTIONE DEL CICLO DI VITA DELLE UTENZE	12
<i>MAT</i>	12
<i>MCC</i>	12
<i>Wilson</i>	12
MONITORAGGIO DELLA CAPACITÀ	13
LOGGING DELLE ATTIVITÀ AMMINISTRATIVE	13
BACK-UP & REDUNDANCY	13
CRITTOGRAFIA BY DEFAULT	14
SEGREGAZIONE ED ISOLAMENTO	15
GESTIONE DELLE RETI VIRTUALI	15
GESTIONE DELLO SVILUPPO SICURO	15
PROTEZIONE DEI DATI DEI CLIENTI	16
ETICHETTATURA DEI DATI DEI CLIENTI	16
CANCELLAZIONE DEI DATI DEI CLIENTI	16
SINCRONIZZAZIONE DEGLI OROLOGI	17
UTILITY PROGRAMS	17
SELEZIONE E MONITORAGGIO DEI FORNITORI	17
CRITERI DI VALUTAZIONE E MONITORAGGIO	17
PIATTAFORME DI FORNITORI CLOUD ATTUALMENTE UTILIZZATE	18
GEOLOCALIZZAZIONE DEI DATI	18
USO RESPONSABILE DELL'AI	18
FUNZIONALITÀ E AFFIDABILITÀ	19
RISERVATEZZA E PROTEZIONE DEI DATI	19
ALLINEAMENTO AL CODICE ETICO DELL'ORGANIZZAZIONE	19
SUPERVISIONE UMANA E CONTROLLO	19
MONITORAGGIO E AUDIT CONTINUO	19
RIFERIMENTI PER I SERVIZI CLOUD DI AI UTILIZZATI	19
CHANGE MANAGEMENT	20

CATEGORIE DELLE MODIFICHE	20
MODALITÀ DI COMUNICAZIONE AI CLIENTI.	20
CESSAZIONE DELLA LICENZA	20
GESTIONE DELLE OPERAZIONI CRITICHE E DOCUMENTAZIONE	21
GESTIONE DELLE VULNERABILITÀ	21
AMBITO ED APPLICAZIONE	21
IDENTIFICAZIONE DELLE VULNERABILITÀ	21
VALUTAZIONE E MITIGAZIONE	21
VERIFICA E MONITORAGGIO	22
COMUNICAZIONE E NOTIFICA	22
INCIDENT MANAGEMENT	22
SEGNALAZIONE DEGLI INCIDENTI E RICHIESTA DI PROVE DIGITALI	22
MODALITÀ DI TRATTAMENTO DEGLI INCIDENTI	22
DISASTER RECOVERY	23
UTILIZZO DEI DATI DEI CLIENTI	24
CONFORMITÀ AI REQUISITI LEGALI	24
CERTIFICAZIONI	24
ULTERIORI REQUISITI LEGALI	24
OBIETTIVI LIVELLO DI SERVIZIO OFFERTO	24
COMUNICAZIONE DA E VERSO I CLIENTI	25
SEGNALAZIONI DI VIOLAZIONE IP DI TERZE PARTI	25
POLICY PER GLI AUDIT DI SECONDA PARTE	25
CONCLUSIONE	25

Introduzione

Questa informativa ha lo scopo di rendere trasparente la gestione dei servizi cloud offerti da 40Factory ai propri clienti.

L'azienda a partire dal 2024, nella sua evoluzione da start-up a scale-up ha affrontato un'attività di consolidamento e miglioramento organizzativa tramite l'implementazione di un Sistema di Gestione Integrato (SGI) per la qualità e la sicurezza delle informazioni, documentato nel suo Manuale del Sistema di Gestione Integrato (MSGI). Tra gli obiettivi per il miglioramento del SGI direzione ha definito **una politica per la sicurezza delle informazioni, trasparente per i propri clienti**, con l'obiettivo di:

- Descrivere le modalità di trattamento e di protezione dei dati personali e non personali.
- Presentare le misure di sicurezza adottate nel sistema di gestione integrato di 40Factory in conformità alle norme adottate dall'organizzazione quali ISO/IEC 9001:2015, ISO/IEC 27001:2022 e ISO/IEC 27017:2021
- Garantire la trasparenza del trattamento dei dati nel rispetto del regolamento UE 2016/679 (GDPR)
- Soddisfare i requisiti del regolamento NIS2 per il supporto dei clienti che ricadono nell'ambito NIS2, nonostante 40Factory sia stato riconosciuto dall'autorità di riferimento europeo per l'Italia ACN come soggetto "non in ambito NIS2" a seguito dell'attività di notifica da parte dell'organizzazione.

Ambito di applicazione

Il documento si applica a tutti i servizi cloud forniti da 40Factory, in qualità di fornitore cloud (*cloud service provider*) per i propri clienti. In questo ambito 40Factory è anche cliente cloud (*cloud service customer*), in quanto utilizza fornitori cloud per i processi interni e per l'erogazione dei servizi offerti.

Principi di conformità

40Factory applica una politica di trasparenza verso i clienti e si impegna a rispettare tutte le normative vigenti oltre agli standard adottati tramite tutte le contromisure necessarie per il rispetto dei requisiti applicabili con un piano di monitoraggio continuo per il mantenimento degli standard adottati ed il loro miglioramento.

I principi alla base dei controlli implementati, con i riferimenti ai requisiti degli standard, sono:

- Struttura di sicurezza, basata su ruoli e responsabilità condivise, con la definizione chiara di responsabilità tra provider, partner e cliente
- Training e formazione del personale tramite un piano di formazione del personale 40Factory volto al rispetto delle norme vigenti alla soddisfazione del cliente e alla sicurezza delle informazioni.

- Monitoraggio dei servizi offerti tramite il tracciamento delle attività, sistemi di reportistica automatica e notifiche automatiche per eventuali anomalie
- Conservazione delle informazioni tramite politiche documentate di retention e cancellazione dei dati.
- Protezione della trasmissione dei dati tramite autenticazione sicura MFA, cifratura tra dispositivi IIoT, API e servizi cloud.
- Selezione dei fornitori cloud tramite la definizione dei requisiti del fornitore, la gestione di contratti inclusi SLA (Service Level Agreement) e DPA (Data Processing Agreement) ed il loro monitoraggio.
- Privacy e protezione dei dati gestiti sia personali che non personali.
- Segregazione dei servizi offerti in ambiente multi-tenant.
- Gestione del change management conforme ai livelli di servizio offerti
- Gestione progetti AI nel rispetto dei requisiti etici e di sicurezza delle informazioni.

Struttura di sicurezza dei servizi basata su ruoli e responsabilità

Modello di responsabilità condivisa

Le parti coinvolte per l'erogazione dei servizi cloud offerti da 40Factory sono:

- **40Factory**: L'organizzazione che eroga il servizio Cloud, in qualità di cloud provider
- **Clienti di 40Factory**: tutti i clienti che sottoscrivono ed utilizzano i prodotti 40Factory. I clienti 40Factory possono utilizzare tali servizi per rivendere servizi e licenze di accesso ai loro clienti finali.
- **Fornitori Cloud di 40Factory**, provider di servizi cloud SaaS utilizzato da 40Factory in qualità di cloud customer. Il fornitore fornisce gli strumenti cloud utilizzati da 40Factory per l'erogazione dei propri servizi.

Segue la tabella di responsabilità, che esplicita per ogni prodotto software il modello di responsabilità condivisa adottato:

Tabella responsabilità MAT CLOUD (SaaS)

Attività	40Factory	Fornitori Cloud	Clienti di 40Factory
Sicurezza fisica e infrastrutturale dei server Cloud		X	
Sicurezza dell'applicazione SaaS	X		
Gestione degli accessi e delle identità			X (tramite risorse Cloud del cliente, 40Factory raccomanda configurazione MFA)
Backup e ripristino dati			X (tramite risorse cloud dei clienti, 40Factory raccomanda configurazione piano di backup)
Backup e ripristino del layer applicativo e delle configurazioni	X	X	
Gestione delle vulnerabilità dell'infrastruttura	X	X	
Gestione delle vulnerabilità dell'applicazione	X		
Conservazione dei dati			X
Disponibilità e continuità operativa	X		X
Supporto tecnico e gestione ticket	X		
Cancellazione dati a termine contratto			X
Cancellazione configurazioni a termine contratto	X	X	

Tabella responsabilità Mat Control center (MCC)

Attività	40Factory	Fornitori Cloud	Clienti di 40Factory
Sicurezza fisica e infrastrutturale dei server Cloud		X	
Sicurezza dell'applicazione SaaS	X		
Gestione degli accessi e delle identità	X		
Backup e ripristino dati	X	X	
Backup e ripristino del layer applicativo e delle configurazioni	X	X	
Gestione delle vulnerabilità dell'infrastruttura	X	X	
Gestione delle vulnerabilità dell'applicazione	X		
Conservazione dei dati	X		X
Disponibilità e continuità operativa	X		
Supporto tecnico e gestione ticket	X		
Cancellazione dati a termine contratto	X		
Cancellazione configurazioni a termine contratto	X	X	

Tabella responsabilità WILSON Cloud (SaaS)

Attività	40Factory	Fornitori Cloud	Clienti di 40Factory
Sicurezza fisica e infrastrutturale dei server Cloud		X	
Sicurezza dell'applicazione SaaS	X		
Gestione degli accessi e delle identità	X		X
Backup e ripristino dati	X	X	
Backup e ripristino del layer applicativo e delle configurazioni	X	X	
Gestione delle vulnerabilità dell'infrastruttura	X	X	
Gestione delle vulnerabilità dell'applicazione	X		
Conservazione dei dati	X		X
Disponibilità e continuità operativa	X		
Supporto tecnico e gestione ticket	X		
Cancellazione dati a termine contratto	X		X
Cancellazione configurazioni a termine contratto	X	X	

Ruoli e responsabilità

Per garantire la qualità e la continuità dei servizi offerto **40Factory ha definito specifici ruoli all'interno della propria organizzazione**. I ruoli definiti dall'organizzazione, come definito nei mansionari, sono:

<i>Ruoli</i>	<i>Contatto</i>	<i>Responsabilità</i>
DPO – Data Protection Officer	dpo@40-factory.com	Monitora la conformità al GDPR, informa e consiglia il titola del trattamento e il responsabile del trattamento dei dati personali, agisce come punto di contatto con le autorità competenti e verso l'esterno.
SSI – Supervisore Sicurezza delle Informazioni (CISO)	info@40-factory.com	Il supervisore per la sicurezza delle informazioni è responsabile dell'attuazione, gestione e controllo delle misure tecniche e organizzative per proteggere i dati e i sistemi informatici dell'organizzazione all'interno.
AI Ethics & Security Lead (CTO)	info@40-factory.com	Il suo compito è monitorare le funzionalità di AI integrate nei prodotti 40Factory allo scopo di essere conformi ai requisiti normative applicabili ed ai requisiti etici definiti dall'organizzazione.
Azure Global Administrator (DOM)	-	È responsabile dell'amministrazione delle risorse Azure create dall'organizzazione a supporto dei servizi interni e per l'erogazione dei servizi offerti.
Wilson 40Factory Administrator	-	Gli amministratori hanno la possibilità di creare nuove istanze per i clienti, modificare i parametri di licenza e monitorare l'utilizzo della soluzione da parte dei clienti.

Tali ruoli sono definiti all'interno dell'*Organigramma aziendale* e della *matrice per la definizione dei ruoli e permessi* del SGI dell'organizzazione.

In base ai ruoli 40Factory provvede alla formazione iniziale e continuativa del personale interno, per garantire il soddisfacimento dei requisiti di qualità e di sicurezza.

Misure tecniche ed organizzative per la sicurezza

I principi alla base delle misure tecniche e organizzative introdotte da 40Factory per implementare la sicurezza delle informazioni estesa ai servizi cloud sono qui elencati e di seguito dettagliati:

1. **Formazione dei dipendenti**
2. **Regolamento aziendale e codice etico**
3. **Politica dei privilegi minimi - User minimum privilege.**
4. **Regole per la gestione degli accessi.**
5. **Gestione ciclo di vita delle utenze**
6. **Monitoraggio delle capacità**
7. **Logging delle attività amministrative**
8. **Backup & Redundancy**
9. **Crittografia by default**
10. **Segregazione e isolamento**
11. **Gestione delle reti virtuali**
12. **Gestione dello sviluppo sicuro**
13. **Protezione dei dati dei clienti**
14. **Etichettatura dei dati dei clienti**
15. **Cancellazione dei dati del cliente**
16. **Sincronizzazione degli orologi**
17. **Utility programs**
18. **Monitoraggio delle risorse**

Formazione dei dipendenti.

40Factory all'interno del sistema di gestione integrato dell'organizzazione definisce su base annuale il budget dedicato **alla formazione di tutto il personale dell'azienda, sia in ambito qualità che sicurezza dell'informazione, anche specifico per la gestione dei servizi cloud.**

Per il personale tecnico viene definito un piano di formazione avanzato strutturato su questi principali temi:

- Sicurezza delle informazioni
- Secure coding
- Secure Development LifeCycle
- Threat modelling

Regolamento aziendale e codice etico

L'azienda ha definito il **regolamento e policy aziendale per la qualità e il regolamento e policy per la sicurezza delle informazioni**. Tutti i dipendenti dell'organizzazione sono informati e tenuti a rispettare il regolamento aziendale per garantire la qualità dei servizi offerti ed il rispetto dei requisiti di sicurezza definiti dall'organizzazione.

Politica dei privilegi minimi - User Minimum privilege

Per garantire la massima sicurezza e integrità dei dati e dei sistemi, **l'azienda adotta una rigorosa politica di *minimum privilege***: ogni utente riceve esclusivamente i permessi strettamente necessari per svolgere le proprie funzioni.

L'assegnazione dei privilegi viene effettuata in base alla mansione ricoperta e definita, responsabilità e necessità operativa; è soggetta a revisioni periodiche da parte del responsabile dell'azienda in modo da assicurare che l'accesso sia sempre adeguato e limitato. Questa pratica riduce in modo significativo la superficie d'attacco, limita l'esposizione a rischi interni ed esterni e contribuisce a mantenere elevati standard di sicurezza e conformità normativa.

Regole per la gestione degli accessi

Specifiche regole di gestione degli accessi informatici si applicano a tutti i servizi cloud con sistemi di autenticazione gestiti all'organizzazione: sono quindi esclusi tutti i permessi e privilegi gestiti su risorse esterne sui tenant cloud dei clienti.

L'azienda ha adottato come **provider per la gestione dell'autenticazione degli utenti** Microsoft EntraID in quanto conforme alle specifiche definite dall'organizzazione; per informazioni specifiche fare riferimento alla documentazione [Microsoft Azure EntraID](#).

L'azienda ha definito **una politica di gestione degli accessi** basata su autenticazione "forte" che verte sui seguenti principi:

- Utenze nominali e non condivisibili anche all'interno dell'organizzazione 40Factory.
- Protezione Multi-Factor-Authentication (MFA) come misura di sicurezza obbligatoria per proteggere l'accesso alle risorse digitali. La MFA è abilitata per tutti i servizi cloud forniti ai clienti, garantendo un livello di protezione adeguato contro accessi non autorizzati. Inoltre, la MFA è attiva su tutte le piattaforme cloud utilizzate internamente ed è vincolante per tutti i dipendenti, indipendentemente dal ruolo o livello di accesso.
- Protezione (MFA) su tenant di proprietà dei clienti: L'organizzazione raccomanda l'impostazione di MFA su tutti i tenant terzi, utilizzati per accedere alla piattaforma Cloud MAT, non sotto il diretto controllo di 40Factory.

Questa politica rafforza il controllo degli accessi, riduce i rischi di compromissione delle credenziali e supporta il rispetto degli standard di sicurezza più elevati.

Il servizi offerti da 40Factory prevedono **la gestione dei privilegi delle utenze dei clienti** per:

- L'assegnazione dei privilegi.
- La revoca delle utenze.
- L'invito di nuovi utenti.

Per dettagli aggiuntivi si può fare riferimento alla documentazione tecnica di prodotto accessibile agli utenti.

Gestione del ciclo di vita delle utenze.

L'organizzazione ha definito il ciclo di vita delle utenze per i prodotti e servizi forniti ai clienti:

MAT

La gestione del ciclo di vita delle utenze è in carico al cliente MAT, dato che il server di autenticazione è di proprietà del cliente. L'organizzazione raccomanda l'utilizzo di modalità di autenticazione forte e una corretta gestione delle utenze.

MCC

Il ciclo di vita delle utenze di MCC segue questo flusso:

- **Creazione delle utenze:** su richiesta del Cliente, il personale 40Factory provvede a invitare gli utenti all'accesso tramite indirizzo e-mail. L'invito avviene sempre sfruttando il sistema di Single Sign-On (SSO) basato su Microsoft Entra ID.
- **Gestione delle credenziali:** poiché viene utilizzato il Single Sign-On, la gestione delle credenziali è demandata all'utente stesso tramite il proprio sistema di gestione accessi.
- **Gestione di ruoli e permessi:** I ruoli e i permessi vengono assegnati dal personale 40Factory per garantire all'utente la visibilità esclusiva sui dati relativi al proprio **sub-tenant**.
- **Revoca delle utenze:** su richiesta del Cliente o in caso di cessazione del contratto, l'invito viene revocato e l'utenza rimossa dalla piattaforma MCC.

Wilson

Il ciclo di vita delle utenze di Wilson segue questo flusso:

- **Creazione delle utenze:** su richiesta del Cliente, il personale 40Factory provvede a invitare gli utenti all'accesso tramite indirizzo e-mail. L'invito avviene sempre sfruttando il sistema di Single Sign-On (SSO) basato su Microsoft Entra ID. In alternativa, l'utente cliente amministratore può invitare utenti nel suo ambiente Wilson, tramite l'apposita interfaccia.
- **Gestione delle credenziali:** poiché viene utilizzato il Single Sign-On, la gestione delle credenziali è demandata all'utente stesso tramite il proprio sistema di gestione accessi.
- **Gestione di ruoli e permessi:** i ruoli e i permessi vengono assegnati dal personale 40Factory per garantire all'utente la visibilità esclusiva sui dati relativi al proprio **sub-tenant**. L'amministratore del Cliente ha inoltre la possibilità di gestire autonomamente i permessi all'interno del proprio sub-tenant tramite interfaccia dedicata.
- **Revoca delle utenze:** su richiesta del Cliente o in caso di cessazione del contratto, l'invito viene revocato e l'utenza rimossa dalla piattaforma Wilson. In alternativa, l'amministratore cliente può rimuovere le utenze dalla piattaforma tramite interfaccia dedicata.

Monitoraggio della capacità

L'azienda ha definito le seguenti **attività per la gestione del monitoraggio dei servizi cloud forniti ai clienti**:

- I Servizi cloud vengono **monitorati su base giornaliera** tramite un'interfaccia che fornisce informazioni su uso delle risorse e raggiungibilità degli endpoint dei servizi
- Oltre al monitoraggio continuo, è presente **un sistema automatico di notifiche push**, che notifica immediatamente ai responsabili gli eventi di: applicazione non raggiungibile, uso eccessivo delle risorse dei servizi o saturazione delle capacità dell'infrastruttura.
- Viene inoltre rilevato automaticamente e notificato **qualunque cambio di configurazione dei servizi gestiti**, al fine di verificare che queste provengano da fonti affidabili e in linea con i processi aziendali

Logging delle attività amministrative

L'organizzazione ha implementato:

- **Sistemi di logging delle attività amministrative** svolte dal personale 40Factory eseguite per l'aggiornamento, la configurazione e la gestione delle risorse necessarie per l'erogazione dei servizi offerti; tali informazioni sono disponibili solo al personale 40Factory.
- **Sistemi di logging delle attività svolte dalle utenze amministrative dei clienti** all'interno delle piattaforme cloud fornite ai clienti; tali sistemi di logging sono disponibili agli amministratori definiti dai clienti.
- **Sistemi di logging delle attività svolte dagli utenti definiti dai clienti** all'interno delle piattaforme cloud fornite ai suoi clienti, tali sistemi di logging sono disponibili agli amministratori definiti dai clienti.

L'accesso ai registri di logging è definito in base ai ruoli e permessi dei singoli utenti.

Back-up & Redundancy

Per l'erogazione dei servizi cloud 40Factory **adotta strumenti di backup & redundancy resi disponibile dalla piattaforma cloud scelta**, Microsoft Azure, per garantire gli obiettivi di livello offerto definiti nel seguito del documento.

Backup policy

L'organizzazione esegue regolarmente **attività di backup su tutti gli ambienti di produzione dei software offerti**, includendo le configurazioni personalizzate dei clienti, i dati da essi caricati e le relative repository software. I backup vengono effettuati con una frequenza elevata e regolare, con intervalli di poche ore tra un salvataggio e l'altro, al fine di minimizzare la perdita di dati in caso di incidenti. Tutti i backup vengono conservati per un periodo minimo di 30 giorni, in modo da garantire una finestra temporale adeguata a eventuali operazioni di ripristino.

L'organizzazione raccomanda ai suoi clienti di configurare il back-up e la ridondanza nei tenant dati sincronizzati alla piattaforma MAT, non sotto il diretto controllo di 40Factory.

Disaster recovery testing

Per assicurare l'efficacia delle procedure di backup e la disponibilità dei dati in caso di necessità, **l'organizzazione effettua test di ripristino con cadenza semestrale**. Queste simulazioni permettono di verificare la coerenza e l'integrità dei dati salvati, oltre a garantire la prontezza operativa della squadra tecnica nell'esecuzione delle attività di recovery.

I back-up seguono la politica di crittografia e gestione dei dati in linea con tutti gli altri dati gestiti dall'organizzazione.

Crittografia by default

L'organizzazione ha adottato le tecnologie crittografiche rese disponibili per l'archiviazione dal provider dei servizi cloud:

I dati di Archiviazione di Azure vengono crittografati e decrittografati in modo trasparente con la [crittografia AES](#) a 256 bit, una delle crittografie a blocchi più solide disponibili, conforme a FIPS 140-2.

La crittografia configurata secondo il principio *security by default*:

- La crittografia di Archiviazione di Azure è abilitata per tutti gli account di archiviazione, compresi Resource Manager e gli account di archiviazione classici.
- La crittografia di Archiviazione di Azure non può essere disabilitata.
- Poiché i dati sono protetti per impostazione predefinita, non è necessario modificare il codice o le applicazioni per sfruttare i vantaggi della crittografia di Archiviazione di Azure. I dati in un account di archiviazione vengono crittografati indipendentemente dal livello di prestazioni (standard o premium), dal livello di accesso (accesso frequente o accesso sporadico) o dal modello di distribuzione (Azure Resource Manager o classico).
- Tutti i BLOB in blocchi, i BLOB di accodamento e i BLOB di pagine nuovi ed esistenti vengono crittografati, inclusi i BLOB nel livello di accesso archivio.
- Tutte le opzioni di ridondanza di Archiviazione di Azure supportano la crittografia e tutti i dati nelle aree primarie e secondarie vengono crittografati quando la replica geografica è abilitata.
- Tutte le risorse di Archiviazione di Azure vengono crittografate, inclusi BLOB, dischi, file, code e tabelle. Vengono crittografati anche tutti i metadati degli oggetti.

Per altre informazioni sui moduli di crittografia sottostanti la crittografia di Archiviazione di Azure, vedere [API di crittografia: nuova generazione](#).

Per informazioni sulla crittografia e sulla gestione delle chiavi per i dischi gestiti di Azure, vedere [Crittografia lato server dei dischi gestiti di Azure](#).

Segregazione ed isolamento

L'infrastruttura 40Factory per la fornitura dei servizi cloud è specificamente definita in modo da garantire, tramite servizi virtualizzati indipendenti, **la segregazione dei dati e delle risorse delle singole istanze dei clienti**. Tali servizi sono gestiti esclusivamente dal Dev Ops Manager che si occupa della creazione del servizio virtualizzato, l'assegnazione delle risorse, il monitoraggio e l'aggiornamento.

Gestione delle reti virtuali

La segregazione delle reti virtuali è adottata come misura di sicurezza nelle soluzioni 40Factory per la separazione delle singole istanze software rilasciate ai clienti.

La configurazione e gestione delle reti virtuali nei nostri ambienti cloud segue principi di sicurezza in linea con le linee guida delle norme.

- Ogni rete virtuale è segmentata per isolare i diversi ambienti (sviluppo, test, produzione) e minimizzare l'esposizione ai rischi.
- L'accesso alle risorse di rete è strettamente controllato tramite firewall dedicato, regole di sicurezza granulari e monitoraggio continuo del traffico.
- Viene applicato il principio del minimo accesso necessario anche a livello di rete, garantendo che i flussi di dati siano autorizzati solo se esplicitamente previsti.
- Le configurazioni sono soggette a revisione periodica per assicurare coerenza con i requisiti di sicurezza, privacy.

Gestione dello sviluppo sicuro

L'organizzazione adotta **un approccio strutturato allo sviluppo del software che integra i principi della sicurezza informatica in tutte le fasi del ciclo di vita dei propri prodotti e servizi digitali**. L'obiettivo è garantire che le soluzioni fornite siano progettate e realizzate per ridurre al minimo i rischi per la sicurezza delle informazioni.

- Lo sviluppo segue un modello **Secure Software Development Lifecycle (SSDLC)**. Ogni fase – dall'analisi dei requisiti alla progettazione, dallo sviluppo alla messa in produzione – prevede controlli di sicurezza dedicati per l'identificazione e la mitigazione delle vulnerabilità.
- Il codice sorgente è sottoposto a **revisione tra pari** e quando opportuno, test dinamici. Queste attività permettono di rilevare tempestivamente errori o vulnerabilità, intervenendo prima della messa in produzione.
- Gli ambienti di sviluppo, test e produzione sono **fisicamente e logicamente separati**. L'accesso a ciascun ambiente è controllato e tracciato, riducendo il rischio di modifiche non autorizzate o contaminazioni tra ambienti.
- Ogni modifica al software è soggetta a un processo di **change management** formalizzato, che prevede documentazione, approvazione e verifica tramite pull request. Le modifiche sono testate in ambienti di staging prima del rilascio finale.
- I team di sviluppo ricevono **formazione continua** sulle migliori pratiche di sviluppo sicuro, incluse le principali vulnerabilità note (es. OWASP Top 10) e le tecniche di mitigazione.

Protezione dei dati dei clienti

La protezione dei dati dei clienti è una priorità fondamentale, garantita attraverso misure tecniche e organizzative avanzate lungo l'intero ciclo di gestione.

- I dati vengono trattati in ambienti cloud sicuri, con processi di segregazione che assicurano la netta separazione tra ambienti di produzione, test e sviluppo.
- In produzione, ogni cliente opera in un contesto logicamente isolato per prevenire accessi non autorizzati e garantire la riservatezza delle informazioni. I dati reali dei clienti non sono mai utilizzati al di fuori dell'ambiente produttivo e per scopi differenti dall'erogazione dei servizi offerti stessi, garantendone la riservatezza.
- Vengono eseguiti test di vulnerabilità periodici su tutti i componenti che trattano dati sensibili, con particolare attenzione alle superfici di esposizione e ai controlli di accesso. Le eventuali vulnerabilità identificate sono gestite secondo procedure strutturate di remediation e tracciabilità. Tutte le attività sono conformi ai requisiti delle normative internazionali applicabili in materia di sicurezza e protezione dei dati.

L'accesso ai dati dei clienti da parte del personale di supporto è concesso esclusivamente per l'erogazione dei **vari servizi svolti**. Nello specifico:

- **MAT Customer data**, permesso gestito dall'*amministratore del sistema del cliente*. L'accesso viene richiesto al cliente esclusivamente per il personale 40Factory coinvolto nello sviluppo del progetto. La procedura di accesso è gestita tramite invito dell'account aziendale del personale 40Factory; quindi, in caso di revoca dell'utenza aziendale i permessi saranno automaticamente revocati.
- **MAT Customer Configuration files**, permesso gestito dall'*MCC Administrator*. L'accesso viene concesso al personale coinvolto nella attività di gestione del progetto e configurazione dei data model del cliente. I permessi di accesso sono gestiti tramite invito dell'account aziendale del personale 40Factory, quindi in caso di revoca dell'utenza aziendale i permessi saranno automaticamente revocati.
- **Wilson Customer data**, permesso gestito da *Wilson Administrator*. L'accesso viene concesso al personale esterno coinvolto nelle attività di gestione del progetto e configurazione dei tenant dei clienti.

Etichettatura dei dati dei clienti

I servizi software cloud offerti da 40Factory prevedono **la gestione delle informazioni caricate dei clienti tramite servizi di etichettatura**. Il dettaglio di queste funzionalità di prodotto è definito nella **documentazione di prodotto rilasciata**, accessibile agli utenti stessi.

Cancellazione dei dati dei clienti

I servizi software offerti da 40Factory prevedono la **gestione della cancellazione dei dati**. Tale gestione prevede la cancellazione dei dati in modalità sicura che non consente di recuperare i dati cancellati né ai clienti stessi, né a 40Factory, né al fornitore dei servizi cloud utilizzati da 40Factory.

Inoltre, il cliente può richiedere la **cancellazione di dati di configurazione dei software, tale attività viene gestita direttamente dal personale 40Factory**. Tale processo di cancellazione prevede la cancellazione sicura dei dati stessi che non potranno quindi più essere recuperati, né dai clienti, né da 40Factory, né dal provider del servizio cloud utilizzato da 40Factory.

Sincronizzazione degli orologi

Tutte le risorse cloud vengono configurate per utilizzare **sistemi di sincronizzazione oraria centralizzati basati su protocolli standard** come NTP (Network Time Protocol). Il tempo di sistema è allineato costantemente con fonti di riferimento attendibili, garantendo coerenza tra i log di sistema, gli eventi di sicurezza e i processi distribuiti. Questa sincronizzazione è fondamentale per l'integrità delle attività di audit, il rilevamento degli incidenti e la correlazione degli eventi tra servizi interdipendenti. **I meccanismi di sincronizzazione sono monitorati e soggetti a controlli periodici** per rilevare eventuali discrepanze o malfunzionamenti. L'accuratezza temporale è parte integrante della postura di sicurezza dell'infrastruttura cloud.

Il *time server* configurato per i servizi cloud è *time.windows.com*.

Utility programs

40Factory non fornisce direttamente utility program per l'accesso ai servizi cloud offerti. Tuttavia, i servizi cloud prevedono **l'utilizzo di API da parte dei clienti**. Tali API sono fornite in conformità con i livelli di sicurezza dei servizi offerti e le operazioni eseguite tramite utility program vengono tracciate dagli applicativi cloud stessi.

I clienti sono responsabili quindi della corretta implementazione degli utility program da loro definiti a protezione dei dati e dei servizi disponibili sulle applicazioni 40Factory.

Selezione e monitoraggio dei fornitori

Criteri di valutazione e monitoraggio

I fornitori utilizzati da 40Factory per i servizi cloud devono soddisfare i requisiti di sicurezza definita dall'organizzazione, garantire la riservatezza dei dati trattati, la geolocalizzazione dei dati conforme ai requisiti definiti e gli SLA contrattuali.

Nella valutazione e selezione dei fornitori e per il loro monitoraggio nel tempo, l'organizzazione ha definito ed applica delle linee guida con un processo e dei criteri di valutazione prestazionali, in modo particolare per i fornitori di servizi cloud.

Il processo segue una sequenza di attività: RISK ASSESSMENT, SCREENING, AGREEMENT, ACCESS CONTROL, MONITORING, TERMINATION.

Nello SCREENING di valutazione dei fornitori di servizi cloud, si applicano i seguenti requisiti:

- CERTIFICAZIONI
- RUOLI E RESPONSABILITA'
- LIVELLO DI SERVIZIO
- CRITTOGRAFIA DEI DATI

- BACKUP E RECOVERY
- AUDIT E LOGGING
- GDPR
- GESTIONE VULNERABILITA' E INCIDENTI
- CONTROLLI SUGLI ACCESSI
- GEOLOCALIZZAZIONE DATI
- PROTEZIONE DEI DATI E PROPRIETA'
- DOCUMENTAZIONE DISPONIBILE E COMUNICAZIONE
- SVILUPPO SICURO

Piattaforme di fornitori cloud attualmente utilizzate

Attualmente i servizi cloud sono erogati tramite l'utilizzo dei servizi delle piattaforme:

Microsoft Azure – di seguito i riferimenti alla documentazione del fornitore in merito ai requisiti indicati:

- [Azure customer data protection](#)
- [Azure GDPR](#)
- [Azure certifications](#)

Atlassian – di seguito i riferimenti alla documentazione del fornitore in merito ai requisiti indicati:

- [Atlassian Certifications](#)

Gitbooks – di seguito i riferimenti alla documentazione del fornitore in merito ai requisiti indicati:

- [Gitbook Certifications](#)

Geolocalizzazione dei dati

L'azienda ha definito le posizioni geografiche ammesse per l'erogazione dei servizi cloud quali:

- Italia
- West Europe

Uso responsabile dell'AI

L'azienda adotta soluzioni di intelligenza artificiale (IA) con l'obiettivo di migliorare l'efficienza dei servizi, ottimizzare i processi e offrire funzionalità evolute ai propri clienti, mantenendo come priorità la trasparenza, la sicurezza e l'etica nell'utilizzo di queste tecnologie.

Tutti i sistemi basati su IA vengono sottoposti a una rigorosa valutazione preliminare per garantirne la conformità con i seguenti criteri fondamentali:

Funzionalità e Affidabilità

Ogni soluzione IA deve rispondere a requisiti chiari in termini di performance, robustezza, spiegabilità dei risultati e tracciabilità delle decisioni automatizzate. I modelli sono selezionati e addestrati in base a obiettivi ben definiti e testati su scenari realistici per valutarne l'efficacia prima della messa in produzione.

Riservatezza e Protezione dei Dati

I dati utilizzati per l'addestramento, l'inferenza o l'elaborazione dei modelli di IA sono gestiti nel pieno rispetto della riservatezza. Non vengono mai utilizzati dati dei clienti senza un'adeguata base legale, consenso esplicito o necessità contrattuale. Tutti i dati sono trattati in conformità con le normative vigenti in materia di protezione dei dati personali, e sono adottate misure di pseudonimizzazione, minimizzazione e segregazione quando applicabile.

Allineamento al Codice Etico dell'Organizzazione

Ogni sistema IA deve essere coerente con i valori fondamentali dell'organizzazione: equità, inclusività, responsabilità, rispetto della dignità umana e non discriminazione. L'utilizzo di algoritmi viene valutato anche sotto il profilo etico, escludendo soluzioni che possano introdurre bias ingiustificati, effetti discriminatori o automatismi non verificabili. È previsto un processo interno di approvazione etica per tutti i progetti IA rilevanti, supportato da un comitato dedicato.

Supervisione Umana e Controllo

Le soluzioni IA adottate non operano mai in modo completamente autonomo in contesti critici. È sempre prevista una supervisione umana responsabile, con possibilità di intervento e verifica delle decisioni automatiche. I clienti hanno il diritto di conoscere quando una funzione o decisione è assistita da IA, secondo i principi di trasparenza algoritmica.

Monitoraggio e Audit Continuo

I modelli e i sistemi IA sono soggetti a monitoraggio continuo e audit periodici per valutare l'efficacia, individuare deviazioni comportamentali, aggiornare i dataset e verificare l'aderenza continua ai criteri di sicurezza e conformità etica.

Riferimenti per i servizi cloud di AI utilizzati

Vengono riportati i riferimenti ai servizi utilizzati dall'organizzazione per la fornitura dei propri servizi di AI.

- [Microsoft Enterprise AI Service of Conduct](#)
- [AI Azure privacy](#)

Change Management

40Factory adotta un processo di change management strutturato per l'aggiornamento, la modifica e la dismissione dei suoi prodotti e servizi software, che è integrato nei processi documentati di Product Lifecycle Management dei sistemi offerti al mercato.

Nello specifico vengono definiti categorie di modifiche e modalità di comunicazione ai clienti.

Categorie delle modifiche

Le tipologie di modifiche definite sui prodotti 40Factory sono:

- Aggiornamento versione applicativo
- Hot fix di sicurezza
- Cessazione della licenza

Modalità di comunicazione ai clienti.

Le comunicazioni riguardanti attività di aggiornamento, modifica avvengono tramite newsletter pianificate verso i singoli clienti. In fase di avvio progetto vengono definiti le caselle mail dei clienti destinatari di tali comunicazioni.

Vengono quindi definite le seguenti tipologie di comunicazione:

- Avvio preventivo attività di aggiornamento, modifica. Contiene informazioni riguardanti data e ora previsto per l'aggiornamento oltre all'eventuale tempo di disservizio.
- Completamento delle attività di aggiornamento o modifica, contiene informazioni sulle modifiche rilasciate e riferimenti a documentazione tecnica.
- Notifica per temporaneo disservizio.
- Notifica per ripristino del disservizio.

Cessazione della licenza

40Factory adotta procedure per la gestione della cessazione dei contratti di licenza, su richiesta del cliente, come definito nel contratto di fornitura. Tali attività sono gestite dal DevOps Manager e dal responsabile IT e il personale 40Factory si occuperà di:

- Rimuovere tutte le utenze e privilegi assegnati al cliente negli ambienti cloud 40Factory.
- Dismettere le risorse allocate al cliente.
- Cancellare in modo sicuro i dati registrati su servizi 40Factory. Tali dati non potranno essere recuperati in alcun modo come definito nelle condizioni contrattuali
- Rimuovere eventuali documenti e file di progetto affidati dal cliente a 40Factory.

Sono state definite le seguenti tempistiche di rimozione dei dati, per consentire al cliente il loro recupero:

- **Dopo 5 giorni ed entro 10 giorni lavorativi:** rimozione dei dati operativi dai sistemi attivi
- **Dopo 30 giorni ed entro 60 giorni lavorativi:** rimozione dei dati dei sistemi di back-up

A seguito della cancellazione dei dati non sarà più possibile in alcun modo il loro recupero.

Gestione delle operazioni critiche e documentazione

40Factory ha definito le modalità di erogazione della documentazione per la gestione delle operazioni critiche da parte dei clienti. Tale documentazione viene fornita per tutti i prodotti 40Factory su piattaforma Gitbook. La documentazione disponibile è accessibile ai seguenti portali:

- [MAT Documentation](#)
- [Wilson documentation](#)
- [MAT Control Center Documentation](#)

A seguito della formazione tecnica "L2 Application Engineer training", erogata da 40Rocket i clienti avranno anche accesso al portale Gitbook "AE Guide". L'accesso a questa documentazione è fornito da 40Factory e riservato al personale scelto dal cliente l'utenza di accesso è personale e non cedibile.

Tale approccio fornisce ai clienti gli strumenti utili per essere consapevoli della gestione delle operazioni critiche nelle applicazioni software fornite da 40Factory.

Gestione delle vulnerabilità

Ambito ed applicazione

La gestione delle vulnerabilità si applica a:

- Sistemi operativi e ambienti server (on-premise e cloud)
- Software e applicazioni sviluppate e/o gestite da 40Factory
- Dispositivi aziendali e asset hardware
- Componenti di terze parti, incluse librerie, plugin, middleware e servizi esterni

Identificazione delle vulnerabilità

L'identificazione delle vulnerabilità avviene attraverso:

- Monitoraggio di fonti autorevoli (Portale ACN)
- Utilizzo di strumenti automatizzati di vulnerability scanning su base periodica
- Segnalazioni da parte di fornitori incaricati nelle procedure di scanning e penetration test

Valutazione e mitigazione

Le vulnerabilità identificate vengono trattate secondo un piano d'azione che può includere:

- Applicazione di patch o aggiornamenti software
- Implementazione di workaround temporanei
- Disabilitazione di funzionalità vulnerabili

- Isolamento dell'asset in attesa della risoluzione

Ogni intervento viene tracciato tramite il sistema di ticketing interno (basato su Jira), indicando data di rilevazione, responsabile assegnato, stato e data di chiusura.

Verifica e Monitoraggio

Successivamente alla risoluzione, vengono eseguite:

- Verifiche tecniche per assicurare che la vulnerabilità sia stata correttamente mitigata
- Scan successivi per confermare l'assenza della vulnerabilità
- Monitoraggio continuo per evitare regressioni

Comunicazione e Notifica

In caso di vulnerabilità critiche che coinvolgano dati o configurazioni di clienti, 40Factory provvede a:

- Informare tempestivamente il cliente interessato
- Fornire dettagli tecnici e indicazioni sulle misure correttive adottate
- Collaborare per eventuali azioni di contenimento da parte del cliente

Incident management

Nel seguito vengono descritte le politiche relative alla gestione incidenti-definite e documentate nel sistema di gestione integrato dell'organizzazione.

Segnalazione degli incidenti e richiesta di prove digitali

L'organizzazione definisce i seguenti canali per la segnalazione degli incidenti:

- [Portale di ticketing Jira Service Desk](#)

All'interno delle relative sezioni di prodotto è definita la categoria inerente agli incidenti di Cybersecurity. È richiesta al cliente la compilazione di tutti i campi obbligatori riguardanti la descrizione dell'incidente, i principi fondamentali impattati dall'incidente e l'impatto organizzativo. Il team di Cybersecurity di 40Factory prenderà in carico la richiesta per risolvere la problematica nel minor tempo possibile ed in linea con gli obiettivi di servizio definiti.

Tramite lo stesso portale, **è possibile richiedere prove digitali legate che possono essere utili per la gestione di un incidente.**

Modalità di trattamento degli incidenti

40Factory ha definito la modalità di trattamento come segue:

- **Gestione degli incidenti:** In caso di disservizi che compromettano la disponibilità dei servizi cloud, la società applica un processo strutturato di gestione degli incidenti. Ogni incidente viene registrato, analizzato e risolto secondo procedure standardizzate, al fine di ridurre al minimo l'impatto sulla continuità del servizio.
- **Classificazione degli incidenti:** Gli incidenti sono classificati in base alla loro gravità, **entro 24 ore lavorative dalla loro segnalazione**, impatto sui servizi e natura dell'evento. Tale classificazione consente di attribuire correttamente le priorità di intervento e le risorse necessarie.
- **Tracciamento e risoluzione:** Tutte le fasi di gestione di un incidente (segnalazione, analisi, risposta, risoluzione) sono tracciate tramite sistema di ticketing interno, indicando responsabilità, impatti e azioni correttive. Nel caso l'incidente comporti un grave impatto alla confidenzialità dei dati, questo verrà comunicato all'autorità nazionale competente (ACN) o al CSIRT designato con queste tempistiche:
 - Entro 24 ore: notifica preliminare
 - Entro 72 ore: notifica dettagliata
 - Entro un mese: relazione finale
- **Miglioramento continuo:** Ogni incidente risolto viene sottoposto a revisione post-evento con l'obiettivo di apprendere dall'esperienza e introdurre eventuali azioni di miglioramento nei processi o nei controlli implementati.

Disaster recovery

Nel caso in cui l'incidente comporti la necessità di attivare il piano di disaster recovery, 40Factory applica le misure previste all'interno della propria strategia di continuità operativa. Tali misure includono:

- **Attivazione del piano di DR:** In seguito alla valutazione dell'incidente da parte del team tecnico e del responsabile della sicurezza, viene attivato il piano di disaster recovery nei casi in cui il ripristino ordinario non sia sufficiente a garantire la ripresa tempestiva delle attività critiche.
- **Ripristino dei dati e dei servizi:** Il ripristino avviene a partire dai backup periodici, che sono verificati regolarmente e conservati secondo quanto definito nel piano di backup. L'obiettivo è garantire il recupero completo dei dati e il ripristino dei servizi entro i tempi definiti nei parametri di Recovery Time Objective (RTO) e Recovery Point Objective (RPO). In ogni caso, il ripristino avviene sempre **entro due giorni lavorativi**.
- **Comunicazione:** Durante la gestione dell'evento, viene garantita una comunicazione tempestiva e trasparente ai clienti e alle parti interessate, secondo i canali e le modalità previste nel piano di crisi aziendale.
- **Verifica e validazione:** Al termine delle operazioni di ripristino, viene effettuata una verifica dell'integrità dei dati e della piena operatività dei servizi. Viene inoltre redatto un report post-evento con l'analisi delle cause, l'efficacia delle azioni adottate e le eventuali aree di miglioramento.

- **Test periodici:** Il piano di disaster recovery viene testato con cadenza almeno semestrale, per garantire l'efficacia e la prontezza del processo in caso di emergenza reale.

Utilizzo dei dati dei clienti

40Factory accede ed utilizza i dati dei clienti allo scopo di:

- Erogare i servizi offerti Ai clienti
- Monitorare l'utilizzo delle proprie applicazione per l'ottimizzazione dei servizi cloud.
- Misurare l'adoption rate delle applicazione da parte dei clienti
- Migliorare i propri prodotti o servizi.

L'organizzazione in nessun modo condividerà i dati utilizzati o una loro elaborazione con soggetti esterni all'organizzazione.

Conformità ai requisiti legali

40Factory è conforme a tutti i requisiti legali territoriali applicabili; inoltre ha definito un sistema di gestione conforme alle norme vigenti e agli standard adottati tramite la definizione e la verificata del rispetto dei seguenti requisiti legali.

Certificazioni

- Norma UNI EN ISO 9001
- Norma UNI CEI EN ISO/IEC 27001
- Norma UNI CEI EN ISO/IEC 27017

Ulteriori requisiti legali

- Regolamento GDPR (UE 2016/679)
- Regolamento NIS2 (DL 138/2024 e UE 2022/2555)
anche se 40Factory è un soggetto non in ambito in quanto fornitore di aziende in ambito.
- Regolamento UE AI Act (UE 2024/1689)
- Regolamento Data Act (UE 2023/2854)

L'azienda analizzando i requisiti legali attualmente in essere non ha evidenziato requisiti specifici sulla tipologia di crittografia implementata per l'erogazione dei servizi offerti.

Obiettivi livello di servizio offerto

Per l'erogazione dei servizi di 40Factory l'azienda ha definito i seguenti obbiettivi, considerando lo stack tecnologico utilizzato dai vari servizi:

Servizio	SLA
----------	-----

MAT Cloud	99,5%
MAT Control Center	99,5%
Wilson Academy	99,5%
Wilson Stand-alone	99,5%

I valori di SLA sono determinati mediante un sistema di monitoraggio continuo delle istanze applicative in produzione. L'uptime viene calcolato come rapporto tra il tempo in cui ogni applicazione risulta operativa e il tempo totale di osservazione, su base annuale. Gli strumenti di monitoraggio impiegati rilevano automaticamente eventuali interruzioni di servizio, oltre a riavvii o problematiche infrastrutturali che possono impattare la fruibilità del servizio.

Comunicazione da e verso i clienti

40Factory comunica attività legate all'erogazione dei servizi offerti ai clienti per le seguenti casistiche e nelle modalità definite:

Tipologia	Canale	Destinatari
Updates MAT	e-mail	Clienti attivi MAT
Disservizio MAT	e-mail	Clienti attivi MAT
Updates Wilson	e-mail	Clienti attivi Wilson
Updates Wilson	e-mail	Clienti attivi Wilson

Segnalazioni di violazione IP di terze parti.

L'azienda ha definito che una violazione di Intellectual Property rientra nel flusso di segnalazione degli incidenti di Cybersecurity, per questo la modalità di segnalazione è in linea con quella definita per la segnalazione incidenti del presente documento:

- [Portale di ticketing Jira Service Desk](#)

Policy per gli audit di seconda parte

40Factory consente ai clienti di eseguire audit di seconda parte solo in seguito ad accordi specifici e previa pianificazione concordata.

È Prevista la firma di un NDA da parte del cliente che può richiedere e consultare il report di audit periodico eseguito dall'azienda.

Conclusione

Questo documento stabilisce una linea guida chiara per la gestione dei contratti di licenza con 40Factory, promuovendo trasparenza, responsabilità e sicurezza delle informazioni.