Principi Kyndryl sulla Sicurezza e Riservatezza dei Dati

kyndryl

1. Definizioni

I termini in maiuscolo utilizzati nel presente documento hanno i significati riportati di seguito o, se non riportati di seguito, i significati forniti nel contratto scritto applicabile tra Kyndryl e il Cliente per i Servizi Kyndryl.

Cliente – è l'entità a cui Kyndryl eroga i Servizi Kyndryl in base a un Documento dei Servizi Kyndryl.

Componenti – sono gli elementi dell'applicazione, della piattaforma o dell'infrastruttura di un Servizio Kyndryl che Kyndryl amministra e gestisce.

Contenuti – consistono in tutti i dati, i software e le informazioni che il Cliente ed i relativi utenti autorizzati forniscono, alle quali forniscano accesso, o che immettono nei Servizi Kyndryl.

DSP – è il presente documento Principi Kyndryl sulla Sicurezza e Riservatezza dei Dati.

Documento dei Servizi Kyndryl – è un Documento d'Ordine e qualsiasi altro documento che sia incorporato in un contratto scritto tra Kyndryl ed il Cliente che affronta i dettagli di uno specifico Servizio Kyndryl.

Servizi Kyndryl – sono (a) offerte di servizi Kyndryl, comprese le offerte di servizi di infrastruttura o applicazioni che Kyndryl fornisce e dedica o personalizza per un Cliente e (b) qualsiasi altro servizio, inclusi consulenza, manutenzione o supporto che Kyndryl fornisce a un Cliente.

Incidente di Sicurezza – è rappresentato da un accesso o da un utilizzo non autorizzato dei Contenuti.

Documento d'Ordine: è un documento che riporta nei dettagli le specifiche delle transazioni, quali ad esempio gli addebiti ed una descrizione del Servizio Kyndryl con le relative informazioni. Alcuni esempi di Documenti d'Ordine comprendono gli Statement of Work (SOW), le Descrizioni del Servizio e le Fatture per un Servizio Kyndryl. È possibile che vi sia più di un Documento d'Ordine applicabile.

2. Panoramica

Le Misure Tecniche e Organizzative (TOMs) fornite nel presente DSP si applicano ai Servizi Kyndryl (inclusi gli eventuali Componenti) solo se Kyndryl ha espressamente accettato di adeguarsi al DSP in un contratto scritto tra Kyndryl e il Cliente. Per chiarezza, tali misure non si applicano laddove il Cliente è responsabile della sicurezza e della privacy o in base a quanto specificato di seguito o in un Documento dei Servizi Kyndryl.

a. Il Cliente è responsabile di determinare se un Servizio Kyndryl è adatto per l'utilizzo da parte del Cliente e di implementare e gestire le misure di sicurezza e privacy per i componenti che Kyndryl non fornisce e gestisce all'interno dei Servizi Kyndryl. Esempi di responsabilità del Cliente per i Servizi Kyndryl includono: (1) la sicurezza dei sistemi e delle applicazioni creati o distribuiti dal Cliente in un'offerta IaaS (Infrastructure as a Service) o PaaS (Platform as a service) che Kyndryl gestisce per un Cliente, e (2) il controllo degli accessi dell'utente finale del Cliente e la configurazione della sicurezza a livello applicativo di un'offerta SaaS (software as a service) che Kyndryl gestisce per un Cliente o di un'offerta di servizio applicativo che Kyndryl eroga a un Cliente.

b. Il Cliente accetta che Kyndryl possa modificare il presente DSP di volta in volta ad esclusiva discrezione di Kyndryl e che tali modifiche sostituiranno le versioni precedenti a partire dalla data in cui Kyndryl pubblica la versione modificata. Nonostante eventuali disposizioni contrarie in qualsiasi contratto scritto tra Kyndryl e il Cliente, le modifiche apportate avranno il fine di: (1) migliorare o chiarire gli impegni esistenti, (2) consentire a Kyndryl di definire la priorità di intervento in relazione a minacce e problemi di sicurezza informatica e sui dati, (3) mantenere l'allineamento con gli standard attualmente adottati e le norme applicabili, oppure (4) fornire ulteriori funzioni e caratteristiche. Le modifiche non degraderanno le funzioni e le caratteristiche di sicurezza o di protezione dei dati dei Servizi Kyndryl.

c. In caso di conflitto tra il presente DSP e un Documento dei Servizi Kyndryl, prevarrà il Documento dei Servizi Kyndryl e se i termini in conflitto sono contenuti in un Documento d'Ordine, verranno identificati come prevalenti sui termini del presente DSP e si applicheranno solo alla specifica transazione.

3. Protezione dei Dati Personali

a. Kyndryl tratterà tutti i Contenuti come riservati, divulgandoli per l'utilizzo solo ai dipendenti Kyndryl, agli appaltatori e ai fornitori (inclusi i subresponsabili) ed esclusivamente per le finalità connesse all'erogazione dei Servizi Kyndryl.

b. Le misure di sicurezza e riservatezza per ciascun Servizio Kyndryl sono implementate in conformità alla sicurezza e riservatezza di Kyndryl attraverso pratiche progettate per proteggere i Contenuti trattati da un Servizio Kyndryl e per mantenere la disponibilità di tali Contenuti ai sensi del contratto tra Kyndryl e il Cliente, inclusi i Documenti dei Servizi Kyndryl applicabili.

c. Ulteriori informazioni sulla sicurezza e sulla riservatezza specifiche di un Servizio Kyndryl possono essere disponibili nel relativo Documento d'Ordine o in altra documentazione standard per fornire assistenza al Cliente in fase di valutazione dell'utilizzo iniziale e in itinere dell'idoneità del Servizio Kyndryl per l'utilizzo da parte del Cliente. Tali informazioni possono includere la prova di certificazioni dichiarate e accreditamenti, informazioni correlate a tali certificazioni e accreditamenti, schede tecniche, FAQ ed altra documentazione generalmente disponibile. Kyndryl indirizzerà il Cliente alla documentazione standard disponibile in caso di richiesta di completamento di questionari su sicurezza e riservatezza preferiti dal Cliente.

4. Policy di Sicurezza

a. Kyndryl manterrà e seguirà le politiche e le procedure di sicurezza IT scritte che sono parte integrante delle attività di Kyndryl e obbligatorie per tutti i dipendenti Kyndryl. Il CIO (Chief Information Security Officer) Kyndryl manterrà la responsabilità e la supervisione esecutiva di tali policy, incluse la governance formale e la gestione della revisione, la formazione dei dipendenti e l'applicazione della conformità.

b. Kyndryl riesaminerà le sue politiche di sicurezza IT almeno una volta all'anno e modificherà tali politiche quando Kyndryl lo riterrà ragionevole per preservare la protezione dei Servizi Kyndryl e dei Contenuti.

c. Kyndryl manterrà e seguirà tutti i requisiti inderogabili di legge relativi all'occupazione rispetto a tutti i nuovi dipendenti assunti ed estenderà tali requisiti alle consociate interamente controllate da Kyndryl. In conformità con i processi e le procedure interne di Kyndryl, questi requisiti saranno periodicamente revisionati e includeranno, a titolo esemplificativo ma non esaustivo, il controllo dei precedenti penali, la prova di convalida dell'identità e ulteriori controlli, qualora ritenuto necessario da Kyndryl. Ciascuna società Kyndryl è responsabile dell'implementazione di questi requisiti nel relativo processo di assunzione, quando applicabile e consentito dalla normativa locale.

d. I dipendenti Kyndryl ogni anno completeranno la formazione su sicurezza e riservatezza di Kyndryl e certificheranno ogni anno di attenersi agli obblighi etici riguardanti le politiche sulla riservatezza, la sicurezza e la condotta aziendale, come stabilito nel documento "Linee Guida Kyndryl sul Comportamento Aziendale" (Business Conduct Guidelines). Ulteriore formazione sarà somministrata a tutte le persone cui viene fornito l'accesso privilegiato ai Componenti in base allo specifico ruolo all'interno delle operazioni e del supporto in relazione al Servizio Kyndryl e in base a quanto richiesto per mantenere la conformità e le certificazioni specificate in qualsiasi Documento dei Servizi Kyndryl pertinente.

5. Conformità

a. Kyndryl manterrà la conformità e l'accreditamento per i Servizi Kyndryl come definito in un Documento dei Servizi Kyndryl.

b. Su richiesta, Kyndryl fornirà la prova della conformità e dell'accreditamento richiesti al punto 5a., quali certificati, attestazioni o rapporti risultanti da audit di terze parti indipendenti accreditate (gli audit di terze parti indipendenti accreditati si svolgeranno con la frequenza richiesta dallo standard pertinente).

c. Kyndryl è responsabile di queste misure di protezione e riservatezza dei dati anche qualora Kyndryl utilizzi un appaltatore o un fornitore (inclusi i subresponsabili) nell'erogazione o nel supporto di un Servizio Kyndryl.

6. Incidenti di Sicurezza

a. Kyndryl gestirà e seguirà le policy documentate di risposta agli incidenti, in conformità con le linee guida del National Institute of Standards and Technology, United States Department of Commerce (NIST) o di equivalenti standard di settore per la gestione degli incidenti di sicurezza informatica e di conformerà alle disposizioni di notifica delle violazioni dei dati stabilite dal contratto tra Kyndryl e il Cliente.

b. Kyndryl esaminerà gli Incidenti di Sicurezza di cui viene a conoscenza e, nell'ambito dei Servizi Kyndryl, definirà e metterà in atto un piano di risposta appropriato. Il Cliente può notificare a Kyndryl una sospetta vulnerabilità o un incidente inviando una richiesta tramite il processo di segnalazione degli incidenti specifico per il Servizio Kyndryl (come indicato in un Documento dei Servizi Kyndryl) o, in assenza di tale processo, inviando una richiesta di supporto tecnico.

c. Al momento della conferma di un Incidente di Sicurezza che sia noto a Kyndryl o per cui si preveda ragionevolmente che vi possano essere conseguenze sulle attività del Cliente, Kyndryl provvederà ad informare il Cliente senza indebito ritardo. Kyndryl fornirà al Cliente le informazioni ragionevolmente necessarie su tali Incidenti di Sicurezza e sullo stato di qualsiasi attività di correzione e ripristino prevista da Kyndryl.

7. Sicurezza Fisica e Controllo Ingressi

a. Kyndryl manterrà un adeguato controllo degli ingressi, quali barriere, punti di ingresso controllati da badge, telecamere di sorveglianza e punti di accoglienza presidiati, per proteggere da ingressi non autorizzati all'interno delle strutture gestite da Kyndryl usate per ospitare i Servizi Kyndryl (data center). I punti di ingresso ausiliari in tali data center come, ad esempio, le aree di consegna e le banchine di carico saranno controllati e isolati dalle risorse informatiche.

b. L'accesso ai data center gestiti da Kyndryl e alle aree controllate all'interno di tali data center sarà limitato in base al ruolo professionale e soggetto ad autorizzazione. Tale accesso verrà registrato e tali registri verranno conservati per non meno di un anno. Kyndryl revocherà l'accesso ai data center gestiti da Kyndryl in questione al momento dell'interruzione della collaborazione con un dipendente autorizzato. Kyndryl si atterrà alle procedure formali di separazione documentate che includono la rimozione tempestiva dalle liste di controllo accessi e la restituzione dei badge di accesso.

c. Qualsiasi soggetto cui sia stata fornita l'autorizzazione temporanea ad accedere ad una struttura di data center gestita da Kyndryl o ad un'area controllata all'interno di tale data center sarà registrato nel momento in cui entra nella sede, dovrà fornire prova dell'identità al momento della registrazione e sarà accompagnato da personale autorizzato. Tutte le autorizzazioni temporanee per l'ingresso, incluse le consegne, saranno pianificate in anticipo e dovranno essere approvate dal personale autorizzato.

d. Kyndryl adotterà precauzioni per proteggere l'infrastruttura fisica del data center gestito da Kyndryl da minacce ambientali, sia in caso di eventi naturali che causati dall'uomo quali, ad esempio, eccessiva temperatura dell'ambiente, incendi, inondazioni, umidità, furti e vandalismo.

8. Controllo Accessi, Interventi, Trasferimenti e Separazione

a. Prima dell'implementazione, Kyndryl riesaminerà l'architettura di sicurezza per i Componenti, incluse le misure per impedire le connessioni di rete non autorizzate a sistemi, applicazioni e dispositivi di rete, in conformità con i propri standard avanzati di segmentazione protetta, di isolamento e di difesa.

b. Kyndryl potrà utilizzare la tecnologia di rete wireless durante la manutenzione e il supporto dei Servizi Kyndryl e dei Componenti associati. Tali reti wireless, se presenti, saranno crittografate e richiederanno l'autenticazione protetta.

c. Per il Servizio Kyndryl, Kyndryl manterrà le misure progettate per separare logicamente e impedire di accedere o esporre il Contenuto a persone non autorizzate. Kyndryl manterrà il necessario isolamento tra i propri ambienti di produzione e non di produzione, e, qualora il Contenuto venga trasferito in un ambiente non di produzione, ad esempio allo scopo di riprodurre un errore al momento della richiesta del Cliente, la sicurezza e la protezione della privacy, nell'ambiente non di produzione, saranno equivalenti a quelle nell'ambiente di produzione.

d. Kyndryl eseguirà la crittografia del Contenuto non destinato alla visualizzazione pubblica o non autenticato durante il trasferimento del Contenuto su reti pubbliche e attiverà l'uso di un protocollo di

crittografia come, ad esempio, HTTPS, SFTP o FTPS, ai fini di un trasferimento sicuro del Contenuto del Cliente verso e dal Servizio Kyndryl su reti pubbliche.

e. Kyndryl eseguirà la crittografia dei Contenuti memorizzati (Content at rest) in base a quanto specificato nel Documento dei Servizi Kyndryl. Se un Servizio Kyndryl include la gestione delle chiavi crittografiche, Kyndryl documenterà le procedure per la generazione, emissione, distribuzione, archiviazione, rotazione, revoca, ripristino, backup, distruzione, accesso e utilizzo di chiavi protette.

f. Se, per erogare i Servizi Kyndryl, Kyndryl richiede l'accesso ai Contenuti, e se tale accesso è gestito da Kyndryl, Kyndryl limiterà l'accesso al livello minimo necessario. Tale accesso, incluso l'accesso di amministratore a tutti i Componenti sottostanti (accesso con privilegi), sarà personale, giustificato dalla funzione, e soggetto ad approvazione e convalida periodica da parte del personale Kyndryl autorizzato in base al principio della separazione dei compiti. Kyndryl manterrà le misure per identificare e rimuovere account ridondanti e dormienti dotati di accesso con privilegi e revocherà tempestivamente tale accesso all'atto di separazione dell'assegnatario dell'account o su richiesta di personale Kyndryl autorizzato come, ad esempio, il responsabile dell'assegnatario dell'account.

g. In conformità con le procedure standard di settore e ove tecnicamente possibile su ciascun Componente, Kyndryl manterrà le misure tecniche applicando il timeout di sessioni inattive, il blocco degli account dopo molti tentativi di accesso sequenziali non riusciti, l'autenticazione complessa mediante password o passphrase, la frequenza di modifica della password e misure che richiedano un trasferimento protetto e la memorizzazione di tali password e passphrase.

h. Kyndryl monitorerà l'utilizzo dell'accesso con privilegi e manterrà le informazioni sulla sicurezza e le misure di gestione degli eventi progettate per: (1) identificare accessi e attività non autorizzati, (2) agevolare una risposta tempestiva e appropriata, e (3) consentire audit interne e di terze parti indipendenti per la conformità con la politica Kyndryl documentata.

i. I log in cui sono registrati l'accesso con privilegi e le attività saranno conservati in conformità con le politiche di Kyndryl. Kyndryl manterrà le misure progettate per proteggere da accessi non autorizzati, modifica e distruzione accidentale o deliberata di tali log.

j. Fatti salvi i limiti delle funzionalità di dispositivi o sistemi operativi, Kyndryl manterrà le protezioni informatiche per i sistemi dei suoi utenti finali che includono, a titolo esemplificativo ma non esaustivo, i firewall di endpoint, la crittografia completa del disco, l'individuazione e la rimozione di malware, il blocco a tempo dello schermo e le soluzioni di gestione endpoint che applichino i requisiti di configurazione della sicurezza e delle patch.

k. Kyndryl cancellerà in modo sicuro i supporti fisici destinati al riutilizzo prima di tale riutilizzo e distruggerà i supporti fisici che non devono essere riutilizzati, in conformità con le linee guida NIST in materia di cancellazione dei supporti.

9. Controllo Integrità e Disponibilità del Servizio

a. Kyndryl provvederà a: (1) eseguire almeno una volta all'anno la valutazione dei rischi per la sicurezza e la privacy dei Servizi Kyndryl, (2) eseguire test di sicurezza e valutazioni di vulnerabilità dei Servizi Kyndryl prima del rilascio in produzione e successivamente almeno una volta all'anno, (3) eseguire test di penetrazione sulle funzionalità e sulle offerte prima del rilascio in produzione e successivamente una volta all'anno, (4) eseguire la scansione automatizzata delle vulnerabilità dei Componenti sottostanti dei Servizi Kyndryl rispetto alle best practice di configurazione della sicurezza del settore, (5) porre rimedio alle vulnerabilità identificate mediante test e scansioni di sicurezza, in base a rischi, sfruttabilità e impatto associati e (6) adottare misure ragionevoli per evitare interruzioni dei Servizi Kyndryl durante test, valutazioni, scansioni e l'esecuzione di attività di riparazione.

b. Kyndryl manterrà le misure progettate per valutare, testare e applicare le patch degli avvisi di sicurezza ai Servizi Kyndryl e ai relativi sistemi, reti, applicazioni e Componenti sottostanti associati ed inclusi nell'ambito dei Servizi Kyndryl. Dopo aver stabilito che una patch degli avvisi di sicurezza è applicabile e appropriata, Kyndryl applicherà la patch a seconda della severità e alle linee guida documentate sulla valutazione del rischio, in base al rating del Common Vulnerability Scoring System (CVSS), ove disponibile. L'implementazione delle patch degli avvisi di sicurezza sarà soggetta alla politica di change management Kyndryl.

c. Kyndryl manterrà le politiche e le procedure progettate per gestire i rischi associati all'applicazione di modifiche ai Servizi Kyndryl. Prima di essere implementate, le modifiche al Servizio Kyndryl, incluse quelle ai relativi sistemi, reti e Componenti sottostanti, saranno documentate in una richiesta di variazione registrata contenente la descrizione e il motivo della modifica, i dettagli e la tempistica

dell'implementazione, una dichiarazione del rischio che indichi l'impatto sul Servizio Kyndryl e i relativi client, i risultati previsti, il piano di ripristino (rollback) e l'approvazione documentata del personale autorizzato.

d. Kyndryl manterrà un inventario di tutti gli asset IT (Information Technology) usati per il funzionamento del Servizio Kyndryl. Kyndryl monitorerà e gestirà continuamente lo stato di salute, compresa la capacità, e la disponibilità dei Servizi Kyndryl e dei Componenti sottostanti.

e. Ciascun Servizio Kyndryl sarà valutato separatamente per i requisiti di continuità operativa e di disaster recovery attraverso un'appropriata analisi dell'impatto aziendale e valutazioni dei rischi intese a identificare e dare priorità alle funzioni aziendali critiche. Ciascun Servizio Kyndryl sarà dotato, nella misura garantita da tale valutazione del rischio, di piani di continuità operativa e di disaster recovery definiti separatamente, documentati, manutenuti e convalidati ogni anno in conformità con le procedure standard di settore. Gli RPO (Recovery Point Objective) e RTO (Recovery Time Objective) di un Servizio Kyndryl, se riportati nel Documento dei Servizi Kyndryl pertinente, saranno stabiliti considerando l'architettura e l'uso previsto del Servizio Kyndryl. I supporti fisici destinati allo storage esterno al sito, se presenti, quali ad esempio supporti che contengono file di backup, saranno criptati prima del trasporto.