Modello di organizzazione, gestione e controllo *ex* D.lgs. n. 231/2001

iVision Tech S.p.A.

Parte speciale 6 “Gestione dei sistemi informatici”

INDICE

CONSIDERAZIONI PRELIMINARI SUL PROCESSO

Il presente documento sintetizza l'insieme dei protocolli diretti a programmare la gestione delle attività e delle decisioni della iVision Tech S.p.A. nel processo "*Gestione dei sistemi informatici*". Il protocollo attiene pertanto all'attività inerente la materia di sicurezza del sistema informatico e telematico e il relativo *risk assessment* è riportato nel documento "mappatura" (cfr. n. 6 della mappatura dei processi).

REATI ASSOCIABILI

Nel paragrafo in questione si individuano le differenti figure di reato che, a seguito dell'attività di *risk assessment*, si ritengono configurabili.

In particolare il processo in oggetto si ritiene a rischio di commissione delle seguenti fattispecie previste dagli **artt. 24-*bis* e 25-*novies*** del Decreto:

Art. 24-bis: Reati informatici

Art. 615-ter c.p. Accesso abusivo ad un sistema informatico o telematico;

Art. 615-quater c.p. Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici;

Art. 615-quinquies c.p. Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;

Art. 617-quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;

Art. 617-quinquies c.p. Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche;

Art. 635-bis c.p. Danneggiamento di informazioni, dati e programmi informatici;

Art. 635-ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;

Art. 635-quater c.p. Danneggiamento di sistemi informatici o telematici;

Art. 635-quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità;

Art. 640-quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica;

Art. 491-*bis* c.p. Falsità in documento informatico;

Art. 482 c.p. Falsità materiale commessa dal privato;

Art.483 c.p. Falsità ideologica commessa dal privato in atto pubblico;

Art.484 c.p. Falsità in registri e notificazioni;

Art. 487 c.p. Falsità in foglio firmato in bianco. Atto pubblico;

Art. 488 c.p. Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali;

Art.489 c.p. Uso di atto falso;

Art. 490 c.p. Soppressione, distruzione e occultamento di atti veri;

Art. 491 c.p. Documenti equiparati agli atti pubblici agli effetti della pena;

Art. 492 c.p. Copie autentiche che tengono luogo degli originali mancanti;

Art. 25-*novies*: Reati in violazione del diritto d'autore

Art. 171 L. 633/1941 co. 1 lett. a) bis Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa;

Art. 171 L. 633/1941 co. 3 Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione;

Art. 171-*bis*, co. 1 Duplicazione, importazione, distribuzione, vendita o detenzione di programmi contenuti in supporti non contrassegnati dalla SIAE;

Art. 171 *ter* L. 633/1941 a fini di lucro abusivamente duplica, mette in vendita opere altrui;

Art. 171 *septies* L. 633/1941 produttori e distributori che a fini di lucro duplica, mette in vendita opere altrui.

POSSIBILI OCCASIONI DI ILLECITO

L'area di rischio, insita in ciascun processo, nel caso di specie può essere rintracciata nelle seguenti fasi:

- definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico;
- gestione degli accessi al sistema informatico degli utenti, dei profili utente e del processo di autenticazione;
- gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni;
- gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni ecc.) e delle attività di inventariazione dei beni;
- acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione);
- monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica;
- gestione degli aspetti infrastrutturali delle transazioni *on-line*.

Le condotte umane tali da concretizzare le fattispecie di reato sopra richiamate sono certamente molteplici e variegate e dunque, a mero titolo esemplificativo e certamente non esaustivo, si riportano taluni casi:

- alterazione del funzionamento di un sistema informatico al fine di procurarsi un ingiusto profitto con l'altrui danno;
- violazione degli obblighi previsti dalla legge per il rilascio del certificato di firma elettronica;
- duplicazione, al fine di trarne profitto, di opere tutelate dal marchio SIAE;
- alterazione documenti informatici;
- accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza;
- installazioni in un numero di copie di un *software* maggiore rispetto al numero di copie effettivamente consentito dalla licenza d'uso del medesimo *software* (comportando un risparmio di spesa);

- vendita e/o utilizzo di *personal computer/smartphone/tablet* con *software* preinstallato (cd OEM) non originale;

- condivisione in rete di *software* coperti da licenza d'uso;

- fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.

SISTEMA DI CONTROLLO

L'attività nel processo dovrà svolgersi nel rispetto delle leggi e regolamenti vigenti, delle norme del Codice Etico, dei valori e delle politiche della iVision Tech S.p.A., delle regole contenute nel Modello e nei protocolli attuativi dello stesso.

Il sistema dei controlli, adottato dall'Organizzazione con riferimento al processo in questione prevede per le attività suindicate:

- principi di controllo "generali", presenti in tutte le attività sensibili;
- principi di controllo "specifici", applicati alle singole attività sensibili.

PRINCIPI DI CONTROLLO GENERALI

I principi di controllo sono stati adottati sulla base delle indicazioni contenute nelle Linee Guida di Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001.

Essi sono stati applicati nell'ambito della realtà organizzativa ed operativa della Organizzazione.

Tali principi sono di seguito indicati:

Esistenza di procedure/linee guida formalizzate: esistenza di specifici documenti volti a disciplinare principi di comportamento e modalità operative per lo svolgimento dell'attività, caratterizzati da una chiara ed esaustiva definizione di ruoli e responsabilità e da un'appropriatezza delle modalità previste per l'archiviazione della documentazione rilevante.

Tracciabilità e verificabilità ex-post delle attività tramite adeguati supporti documentali/ informatici: verificabilità, documentabilità, coerenza e congruenza di operazioni, transazioni e azioni, al fine di garantire un adeguato supporto documentale che consenta di poter effettuare specifici controlli.

Separazione dei compiti: l'esistenza di una preventiva ed equilibrata distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi anche all'interno di una stessa Unità Organizzativa, idonei ad evitare commistione di ruoli potenzialmente incompatibili o eccessive concentrazioni di responsabilità e poteri in capo a singoli soggetti.

Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate: l'attribuzione di poteri esecutivi, autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali assegnate nell'ambito dell'attività descritta, oltre che chiaramente definiti e conosciuti all'interno della Organizzazione.

PRINCIPI DI CONTROLLO SPECIFICI

Ogni attività svolta con l'ausilio del mezzo informatico deve avvenire nel rispetto della normativa vigente, della normativa in materia di diritto d'autore, *copyright* e trattamento dei dati personali, nonché nel rispetto di tutta la normativa nazionale ed internazionale concernente l'utilizzo dei mezzi informatici. A tal fine la iVision Tech S.p.A. ha adottato una specifica procedure che segue.

GESTIONE DELLE POSTAZIONI INFORMATICHE

Funzioni coinvolte

RIT - Responsabile Ufficio Sistemi Informatici;

IT - Ufficio Sistemi Informatici.

Articolazione delle attività

Per gestire le postazioni informatiche, RIT provvederà unitamente a IT a:

- catalogare tutte le macchine presenti evidenziando il *software* caricato, indicando l'eventuale data di scadenza delle singole licenze;
- introdurre protezioni in grado di limitare l'accesso ai siti *internet* contenenti materiale sensibile (pedopornografico; terrorismo; violenza; *file torrent,* etc);
- introdurre protezioni in grado di impedire l'utilizzo di *software* per il *download* di documenti, disegni, modelli e *software*;
- dotare ogni postazione informatica di una *password* personalizzata abbinata allo *username* dell'utente, predisponendo la registrazione di ogni accesso;
- dotare ogni postazione informatica abilitata all'accesso ad *internet* di *password* personalizzata abbinata allo *username* dell'utente, predisponendo la registrazione di ogni accesso;
- dotare ogni postazione informatica di meccanismi di *stand-by* protetti da *password* abbinata a *username*, al fine di evitare l'utilizzo indebito della macchina in caso di allontanamento temporaneo dell'utente;
- in caso di PC utilizzati da più utenti, saranno predisposti più *account* di accesso, personalizzati con distinti *username* e *password*; se ciò non fosse possibile, sarà predisposto un registro di turnazione ovvero in altra forma ritenuta più idonea, dalla quale sia possibile risalire in base alla fascia oraria di utilizzo all'utente che in quel momento aveva accesso alla postazione informatica;

- imporre la modifica obbligatoria delle *password* almeno semestralmente;

RIT, inoltre, si occuperà di:

- far compilare e accettare formalmente a tutti gli assegnatari della dotazione informatica *hardware* e *software* la "*scheda di presa in carico*" (in calce al presente paragrafo) ove, previa elencazione di tutta la strumentazione *hardware* e *software* fornita, saranno descritte le condizioni d'uso che tutto il personale si impegna a rispettare;

- prevedere, nella scheda di presa in carico:

    - l'obbligo di utilizzare il *pc* per le sole esigenze di servizio e non anche quelle personali;

    - l'obbligo di non cedere, in nessun caso, neppure in via temporanea, l'uso del *pc* a terzi, né a titolo gratuito né a titolo oneroso, tenendo, in particolare, segreta la *password* per il collegamento da remoto alla rete dell'organizzazione, laddove previsto;

    - il divieto di installare *software* non forniti dalla iVision Tech S.p.A. anche se distribuiti gratuitamente;

    - il divieto di divulgare la *password* tra le risorse dell'ente;

    - l'obbligo di conservare e custodire con cura e con la massima diligenza il *pc* provvedendo alla restituzione dello stesso nello stato attuale, salvo il normale deterioramento;

    - l'obbligo di comunicare con la massima tempestività l'eventuale smarrimento e/o furto del *pc* informando in ogni caso la iVision Tech S.p.A. circa la natura e l'entità dei dati in esso memorizzati;

    - l'obbligo di comunicare gli eventuali malfunzionamenti del *pc* mettendo in qualsiasi momento il *pc* stesso a disposizione della iVision Tech S.p.A. o di un suo incaricato per ogni operazione di manutenzione e/o riparazione che dovesse essere ritenuta necessaria;

    - alla riconsegna del materiale far compilare e sottoscrivere la scheda di restituzione della dotazione informatica, con elenco dei beni, stato d'uso (funzionante e non), ed espresso divieto di criptare, riservare, rendere comunque inutilizzabili i dati contenuti nel pc oggetto di riconsegna.

iVision Tech S.p.A.
Via Alberico Albricci 8, 20122 Milano
P.IVA 05103540265

Verbale di presa in carico della strumentazione informatica.

La iVision Tech S.p.A. consegna al dipendente sig./sig.ra _____

la seguente strumentazione informatica costituita dai *device*, di seguito meglio individuati:

Dispositivo	Marca	N° serie

I dispositivi indicati hanno installati i seguenti software

Dispositivo	Software installati	Scadenza licenza

Tali dispositivi sono consegnati al dipendente per uso esclusivamente professionale e non personale.

La risorsa, con la sottoscrizione della presente, si impegna a:

- modificare le *password* di accesso al dispositivo e al sistema operativo ogni semestre;
- non divulgare le *password* a terzi, neppure ai colleghi;
- utilizzare i *device* per le sole esigenze di servizio e non anche quelle personali;
- non cedere, in nessun caso, neppure in via temporanea, l'uso del *device* a terzi, neppure ai colleghi;
- non installare *software* non forniti dalla iVision Tech S.p.A. anche se distribuiti gratuitamente;
- non effettuare il *download* di *software* senza la preventiva autorizzazione da parte dell'organizzazione;
- non visitare siti *internet*, portali, piattaforme e/o *forum* con contenuti illegali (pedopornografio; terrorismo; violenza);
- conservare e custodire con cura e con la massima diligenza i *device* provvedendo alla restituzione dello stesso nello stato attuale, salvo il normale deterioramento, non appena richiesto dall'organizzazione;
- comunicare con la massima tempestività l'eventuale smarrimento e/o furto del *pc* informando in ogni caso la iVision Tech S.p.A. circa la natura e l'entità dei dati in esso memorizzati;
- comunicare gli eventuali malfunzionamenti del *device* all'organizzazione mettendolo in qualsiasi momento a disposizione il bene per ogni operazione di manutenzione e/o riparazione che dovesse essere ritenuta necessaria.

La risorsa sig./sig.ra _____

Firma _____

CESSAZIONE DEL RAPPORTO DI LAVORO E/O DI COLLABORAZIONE

Funzioni coinvolte

RIT - Responsabile Ufficio Sistemi Informatici;

IT - Ufficio Sistemi Informatici.

Articolazione delle attività

Ogni risorsa della iVision Tech S.p.A., al termine del rapporto di lavoro e/o di collaborazione, provvederà a:

- restituire ogni dispositivo ricevuto;
- non effettuare copie e/o *backup* di dati e/o informazioni di pertinenza della iVision Tech S.p.A.;
- consegnare ogni documento in originale e/o in copia di pertinenza della iVision Tech S.p.A.;
- collaborare con IT e RIT al fine di migrare i contenuti della propria posta elettronica ad altri *account* di pertinenza dei colleghi;
- collaborare con IT e RIT al fine di chiudere il proprio *account* di posta elettronica o di prevederne la chiusura, entro un periodo di tempo limitato, in modo da permettere, a eventuali mittenti, di conoscere gli indirizzi *mail* a cui inoltrare le proprie richieste.

PROTEZIONE DEI SISTEMI INFORMATICI O TELEMATICI DA EVENTUALI DANNEGGIAMENTI

Funzioni coinvolte

RIT - Responsabile Ufficio Sistemi Informatici;

IT - Ufficio Sistemi Informatici.

Articolazione delle attività

A seguito dell'entrata in vigore, in data 5.04.2008, della Legge 18 marzo 2008 n. 48, attuativa della Convenzione del Consiglio d'Europa in tema di criminalità informatica, ai fini della prevenzione dei reati così introdotti ai sensi del D.Lgs. n. 231/2001, in uno con quanto dettato sopra, IT e RIT opereranno al di fine di:

- individuare le persone fisiche abilitate all'accesso al *server* dell'organizzazione;
- individuare le persone fisiche abilitate all'accesso ai sistemi informatici e alle banche dati;
- esplicitare i sistemi informatici e telematici e le relative banche dati accessibili, vietando l'accesso a quelli non espressamente indicati;
- prevedere un piano di *backup* periodicamente aggiornato e testato;
- esplicitare i limiti di azione delle persone all'interno dei sistemi telematici e delle banche dati, in particolare:

- indicare specificamente l'attività che deve essere svolta;
- vietare esplicitamente ogni attività estranea all'operatività dell'organizzazione;
- evidenziare e vietare quei comportamenti atti ad integrare i reati in materia informatica e telematica;
- attenersi alle regole dettate dal proprietario del sistema telematico e/o della banca dati.

- nominare un amministratore di sistema come da indicazioni del Garante della tutela dei dati personali (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008).

I predetti punti di controllo saranno applicate ai server, sistemi informatici, telematici e relative banche dati in uso sia presso la iVision Tech S.p.A. che presso eventuali clienti e/o parti terze.

TUTELA DEL DIRITTO D'AUTORE

Funzioni coinvolte

RIT - Responsabile Ufficio Sistemi Informatici.

Articolazione delle attività

La risorsa interessata, nel caso si ravvisi la necessità di apposito programma non già caricato sulla macchina in uso (previa regolare licenza), inoltrerà richiesta a RIT per l'acquisto del *software*, il quale provvederà nel rispetto del protocollo "*Approvvigionamento di beni e servizi*" del presente modello di organizzazione, gestione e controllo.

RIT aggiornerà tempestivamente il catalogo dei sistemi informatici in uso, a seguito di implementazione degli stessi in ragione dell'acquisto di nuovi programmi.

È fatto divieto a ciascun operatore di postazione informatica scaricare da *internet* programmi, *files* od applicazioni, anche se catalogate come "*free download*".

TUTELA DI MARCHI, BREVETTI E PROPRIETÀ INDUSTRIALE

Funzioni coinvolte

AD - Amministratore Delegato

Articolazione delle attività

Le risorse della iVision Tech S.p.A., impegnate all'interno degli Uffici Tecnici, e nella disponibilità di documentazione (grafica, narrativa, descrittiva, formule, disegni, sia in formato digitale che cartaceo) afferente a marchi, brevetti e alla proprietà industriale, tanto della iVision Tech S.p.A. quanto dei lei clienti, sottoscriverà l'accordo di riservatezza consegnato da AD ed a cui dovrà adempiere sia in corso d'opera che al termine del rapporto professionale con l'organizzazione.

DATA BREACH

Il c.d. *data breach* è una violazione dei sistemi informatici che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dalla iVision Tech S.p.A.. La violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Alcuni possibili esempi di *data breach* sono:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, *virus*, *malware*, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Il titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Nel caso in cui una delle risorse della iVision Tech S.p.A. e/o anche un collaboratore, consulente, *partner*, fornitore venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.
La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:
1. rilevazione e segnalazione della violazione dei dati personali;
2. raccolta delle informazioni sulla violazione e comunicazione della violazione;

3. valutazione del rischio;

4. individuazione delle azioni correttive;

5. comunicazione delle valutazioni effettuate e delle azioni da intraprendere.

Attività	Chi	A chi	Quando	Come
Rilevazione e segnalazione eventuale *data breach*	- tutto il personale - collaboratori - fornitori - responsabili	Responsabile della struttura di appartenenza	Appena se ne viene a conoscenza	Via mail o telefono
Raccolta delle informazioni sulla violazione e comunicazione del data breach	Il soggetto che ha rilevato la violazione dei dati assieme a RIT	Titolare del Trattamento	Entro 24 ore	Modulo per raccolta informazioni
Valutazione del rischio	Titolare del Trattamento - RIT		Appena ricevuta la comunicazione	Metodologia di valutazione del rischio connesso alla violazione
Individuazione delle azioni correttive	Titolare del Trattamento - RIT		Appena terminata la valutazione di impatto	Analizzando i risultati della valutazione del rischio
Notifica della violazione (se necessaria)	Titolare del Trattamento	Al Garante	Entro 72 ore dalla rilevazione	Modulistica predisposta dal Garante
Comunicazione agli interessati (se necessaria)	Titolare del Trattamento	Interessati (le persone fisiche coinvolte)	Nei termini indicati nella valutazione del rischio	Mail, posta oppure nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, si potrà utilizzare una comunicazione pubblica, (es. sito web, radio, giornale).
Documentazione delle violazioni	RIT - o consulente esterno ove nominato	Titolare del Trattamento	Appena concluse le fasi precedenti	Inserimento dati nel Registro delle violazioni attraverso apposita procedura informatica

\

RAPPORTI CON L'ORGANISMO DI VIGILANZA

Tutti i soggetti coinvolti nel processo dovranno dare tempestiva comunicazione all'Organismo di Vigilanza, di eventuali significativi scostamenti dai flussi procedurali o di eventuali criticità significative e rilevanti ai fini dei modello organizzativo previsto dal D.Lgs. n. 231/2001.

Il canale informativo è l'indirizzo di posta elettronica odv@ivisiontech.eu.

L'OdV ha facoltà di:

- prendere visione di tutti i documenti concernenti la gestione delle postazioni informatiche;
- prendere visione del registro delle postazioni informatiche condivise;
- accedere ai documenti telematici inviati, al fine di verificare la loro coincidenza con gli eventuali atti originali cartacei ovvero con i dati sulla base dei quali è stato predisposto il documento telematico;
- verificare la corrispondenza tra i programmi dichiarati come installati sul PC e quelli effettivamente presenti;
- verificare le licenze dei programmi installati sui PC.

L'OdV riceverà, con cadenza semestrale, le seguenti informazioni:

- numero di amministratori di sistema abilitati/disabilitati;
- numero di incidenti di intrusione ed eventuali criticità rilevate;
- numero di spam/virus rilevati nel periodo;
- numero di interruzioni ai servizi telematici e relative cause;
- nuove licenze *software* acquistate/scadute/rinnovate;
- *software* installato e non licenziato;
- operazioni effettuate in deroga alle procedure e/o promanate direttamente da apicali;

Eventuali contenziosi e/o criticità emerse saranno invece comunicate all'OdV nell'immediatezza dei fatti.

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza attua le procedure di controllo previste dal Modello di Organizzazione e Gestione ed effettua periodicamente controlli a campione sulle attività

potenzialmente a rischio di reato, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole del Modello e, in particolare, alle procedure interne in essere. Il medesimo Organismo provvederà ad esaminare e verificare tutte le segnalazioni ricevute, analizzare i report provenienti dai responsabili di funzione, nonché predisporre un piano di verifiche periodico da integrare in relazione a specifiche esigenze. A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione.