MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

PARTE SPECIALE

4

Reati informatici

Sommario

1. I reati informatici (artt. 24 e 24-*bis* del D. Lgs. 231/2001)

I reati informatici vengono individuati, quali reati-presupposto della responsabilità *ex* D.lgs. n. 231/2001, negli artt. 24 e 24-*bis* del decreto *de quo*. Essi possono essere commessi all'interno della Fondazione, ma anche nell'ambito dei rapporti che la Fondazione intrattiene con i clienti e con le parti correlate. Compiutamente descritte nell'Allegato 1 del Modello, le fattispecie di interesse per la Fondazione sono le seguenti.

1.1. Frode informatica in danno dello Stato o di un ente pubblico (art. 640-*ter* c.p.)

L'art. 640-*ter* c.p. dispone:

> *"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*
>
> *La pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.*
>
> *Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età".*

1.2. Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.)

L'art. 615-*ter* c.p. dispone:

"*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

1.3. Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.)

L'art. 615-*quater* c.p. dispone:

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro

5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater".

1.4. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.)

L'art. 615-*quinquies* c.p.:

"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329."

1.5. Danneggiamento di informazioni, dati e programmi informatici, anche di quelli utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (artt. 635-*bis* e *ter* c.p.)

L'art. 635-*bis* c.p. dispone:

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

L'art. 635-*ter* c.p. dispone:

"Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei

programmi informatici, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

1.6. Danneggiamento di sistemi informatici o telematici, inclusi quelli di pubblica utilità (artt. 635-*quater* e *quinquies* c.p.)

L'art. 635-*quater* c.p. dispone:

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

L'art. 635-*quinquies* c.p. dispone:

"Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

1.7. Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati (art. 171-*bis* co. 2° Legge n. 633/1941)

L'art. 171-*bis* co. 2° Legge n. 633/1941 dispone:

"Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in

violazione delle disposizioni di cui agli articoli 64 quinquies e 64 sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102 bis e 102 ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità."

1.8. Abusiva duplicazione, per trarne profitto, di programmi per elaboratore (art. 171-*bis* co. 1° Legge n. 633/1941)

L'art. 171-*bis* co. 1° Legge n. 633/1941 dispone:

"Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità".

2. Mappa aziendale delle aree a rischio commissione dei reati informatici

Le macroaree di attività considerate maggiormente a rischio in relazione ai reati informatici sono ritenute le seguenti:

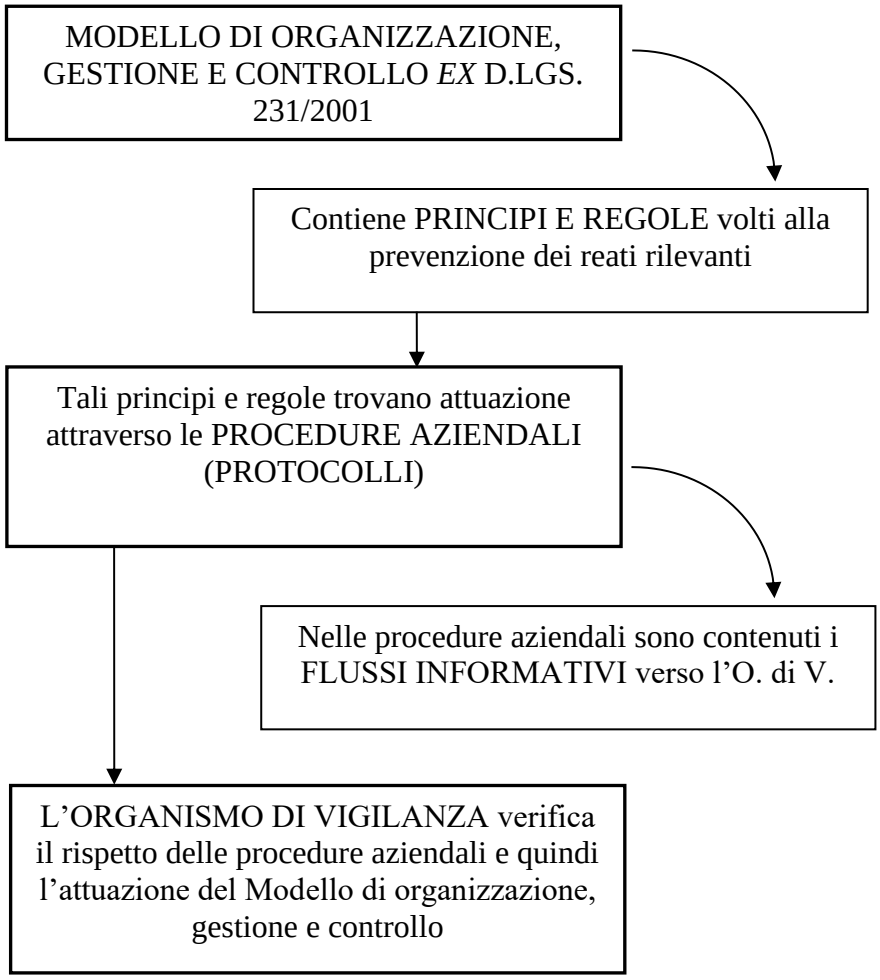
- **Ordinaria e straordinaria amministrazione.**

Nell'ambito dell'area "Ordinaria e straordinaria amministrazione" i processi (o attività) sensibili sono risultati:

- Gestione sistemi informatici.

Per ciascuna macro-area è stata elaborata una mappatura del rischio.

Peraltro, merita di essere evidenziato che ad ogni macroarea corrispondono una o più procedure aziendali, il rispetto delle quali da parte degli esponenti aziendali costituisce lo strumento attraverso il quale l'azienda si adegua al Modello organizzativo adottato, attraverso il seguente schema:



3. Principi generali di comportamento.

La presente Parte speciale si riferisce a comportamenti posti in essere dai membri del Consiglio di amministrazione, dal Direttore generale, dalle singole funzioni responsabili a seconda dei casi coinvolte nelle attività specificamente esposte al rischio di commissione dei reati di cui alla presente Parte speciale, dai dipendenti operanti nelle aree di attività a rischio, nonché da collaboratori esterni e *partner*.

La presente Parte speciale prevede l'espresso divieto – a carico degli esponenti aziendali, in via diretta, ed a carico dei collaboratori esterni e *partner*, tramite l'apposizione di apposite clausole contrattuali – di:

- realizzare condotte tali da integrare le fattispecie di reati informatici (artt. 24 e 24-*bis* del Decreto);
- porre in essere comportamenti che, sebbene non risultino idonei ad integrare, come tali, fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente divenirlo;
- porre in essere qualsiasi situazione di conflitto di interessi nella Fondazione in relazione a quanto previsto dalle suddette ipotesi di reato;
- tacere, verso l'Organismo di vigilanza, l'esistenza eventuale di una circostanza di conflitto di interessi con la Fondazione da parte dei soggetti in posizione apicale, soggetti che invero rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, ovvero ancora esercitanti, anche di fatto, la gestione e il controllo dell'ente stesso.

Nella gestione delle attività in oggetto, tutti i Destinatari del presente Modello dovranno garantite le seguenti azioni preventive di carattere generale:

a) Segregazione delle attività: separazione delle attività in modo tale che nessuno possa gestire in autonomia tutto lo svolgimento di un processo.

b) Norme/Circolari: disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.

c) Poteri autorizzativi e di firma: coerenti con le responsabilità organizzative e gestionali assegnate (prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese) e chiaramente definiti e conosciuti all'interno della Fondazione.

d) Tracciabilità: verificabilità *ex post* del processo di decisione, autorizzazione e svolgimento dell'attività sensibile, anche tramite appositi supporti documentali e, in ogni caso, dettagliata disciplina della possibilità di cancellare o distruggere le registrazioni effettuate.

e) Formazione: la Fondazione garantisce la formazione continua ai soggetti che a vario titolo insistono sui processi in esame.

4. Presidi di controllo specifici

È necessario assicurare che siano formalmente tracciabili e documentati (anche ai fini delle attività di verifica di competenza dell'Organismo di Vigilanza) i seguenti presidi di controllo ritenuti maggiormente rilevanti al fine di mitigare potenziali rischi-reato ai sensi del D.lgs. 231/01:

- tutte le comunicazioni della Fondazione devono essere tracciate;
- devono essere previste riunioni periodiche tra il Direttore generale e l'Organismo di vigilanza per verificare l'attuazione delle regole di gestione;
- deve essere garantita la chiara definizione dei dati e delle informazioni che devono essere forniti al Direttore generale da parte dei Responsabili di ogni singola funzione aziendale;
- occorre mantenere un efficace sistema di sicurezza informatica, in particolare attraverso
    a. la protezione dei sistemi e delle informazioni dai potenziali attacchi, attraverso l'utilizzo di strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attacchi, nonché
    b. la garanzia della massima continuità del servizio;
- l'assegnazione e la gestione delle credenziali di autorizzazione personale (*username* e *password*) e delle credenziali di accesso alle diverse sezioni del sistema informatico della Fondazione e i termini di validità delle medesime devono essere stabilite secondo idonee policy aziendali;
- l'accesso alle diverse sezioni del sistema informatico della Fondazione e a eventuali dati, informazioni, sistemi informatici e telematici cui la Fondazione abbia accesso è riconosciuto a dipendenti, collaboratori, consulenti e partner nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico e coerentemente con gli obiettivi aziendali;
- ogni singolo utente è personalmente responsabile riguardo all'utilizzo del sistema informatico della Fondazione, inclusi eventuali dati, informazioni, sistemi

informatici e telematici cui la Fondazione abbia accesso, nell'ambito dei presidi posti dalla Fondazione a tutela della sicurezza, integrità e riservatezza dei dati;

- è vietato ad amministratori, dipendenti, collaboratori, consulenti e partner, che a vario titolo abbiano accesso alla rete aziendale, di installare propri software che non rientrino nello scopo per cui il sistema informatico è stato assegnato all'utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale;
- è vietato ad amministratori, dipendenti, collaboratori, consulenti e partner di operare in maniera illecita su sistemi informativi altrui al fine di sottrarre fraudolentemente dati o informazioni riservate o sensibili;
- l'installazione di nuove apparecchiature IT, strutture e procedure deve essere formalmente approvata dal Responsabile d'area. L'approvazione deve includere il parere favorevole del Responsabile della sicurezza Informatica;
- il processo di definizione ed approvazione di nuove strutture IT, e della loro modifica, deve essere sempre formalizzato. Il processo di approvazione comprende un'analisi, effettuata dal settore aziendale sulla sicurezza informatica, avente come finalità quella di assicurare che le nuove tecnologie non presentino lacune sotto il profilo della sicurezza e non influenzino negativamente i sistemi e le procedure attualmente presenti;
- è vietato ad amministratori, dipendenti, collaboratori, consulenti e partner, che a vario titolo abbiano accesso alla rete aziendale, di installare nella rete propri software che possano impedire o interrompere o danneggiare le comunicazioni informatiche aziendali ovvero l'intero sistema informatico aziendale;
- qualora si verifichino circostanze non regolamentate, che si prestano a dubbie interpretazioni, tali da originare difficoltà nell'operatività dell'attività, è obbligo di tutti i soggetti coinvolti di ricorrere al Responsabile dell'area di riferimento che, sentito l'OdV, assume le decisioni del caso.

Occorre, inoltre, dare debita evidenza alle operazioni svolte nelle aree a rischio.

A tal fine, il Direttore generale e i responsabili delle funzioni all'interno delle quali vengono svolte operazioni a rischio divengono responsabili delle aree a rischio-reato di ogni singola operazione a rischio da loro direttamente svolta o attuata nell'ambito della funzione a loro facente capo.

Detti responsabili:

- divengono i soggetti referenti dell'operazione a rischio;
- sono responsabili in particolare dei rapporti con i pubblici ufficiali, per le attività con essi svolte.

5. Gestione dei processi incidenti sul rischio reati informatici

Occorre a questo punto dare debita evidenza delle operazioni svolte nelle aree a rischio, con particolare riferimento alla specifica attività aziendale, al fine di individuare i presidi utili alla mitigazione dei rischi di commissione dei c.d. reati informatici.

Le schede che seguono sono composte da sei riquadri: **attività sensibile** (macroarea relativa alle "attività a rischio commissione reati informatici"); **reato** (reati "rilevanti", alla cui commissione è esposta la Fondazione); **finalità della condotta** (elencazione a titolo esemplificativo e non esaustivo); **esempi di modalità di realizzazione della condotta** (elencazione a titolo esemplificativo e non esaustivo); **attività di controllo** (principi e regole contenuti nel Modello e nelle Procedure aziendali, etc. per prevenire la commissione dei reati indicati); **fattore qualificante il controllo** (strumento aziendale - Modello, Procedure aziendali, etc. - in cui sono contenute le regole il cui rispetto esonera l'azienda dalla responsabilità amministrativa dell'ente per uno dei fatti - reato indicati).

Attività sensibile: gestione sistemi informatici
Reati: ● Frode informatica in danno dello Stato o di altro Ente pubblico; ● Accesso abusivo ad un sistema informatico o telematico; ● Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- Danneggiamento di informazioni, dati e programmi informatici (tra cui quelli utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità);
- Danneggiamento di sistemi informatici o telematici (tra cui quelli di pubblica utilità);
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati;
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore

Finalità della condotta: ottenere vantaggi indebiti per la Fondazione

Esempi di modalità di realizzazione della condotta: 1) Il DG, con il supporto della Funzione interessata, alterando il funzionamento di un sistema informatico pubblico, riesce a modificare dei dati in esso contenuti, facendo risultare indebitamente la Fondazione come beneficiaria di erogazioni pubbliche che la stessa non sarebbe legittimata ad ottenere. 2) Il DG, con il supporto della Funzione interessata, riesce ad introdursi nel sistema informatico del Comune di Roma, violando le misure di sicurezza del predetto sistema (es: cracking delle password). 3) La Funzione interessata di Fondazione Bioparco di Roma, utilizzando un software adatto a portare a termine un attacco nei confronti del sistema informatico del Comune di Roma, riesce ad entrare in possesso delle chiavi di accesso di detto sistema. 4) La Funzione interessata di Fondazione Bioparco di Roma, allo scopo di penetrare all'interno del sistema informatico del Comune di Roma, si procura un software adatto a superare le misure di sicurezza predisposte a tutela del sistema stesso. 5) La Funzione interessata di Fondazione Bioparco di Roma, penetrata all'interno del sistema informatico del Comune di Roma, elimina in

modo permanente dal sistema ingenti quantità di dati in modo tale da impedire definitivamente (o, quantomeno, bloccare temporaneamente) l'operatività del sistema. 6) La Funzione interessata di Fondazione Bioparco di Roma, superando i sistemi di protezione del sistema informatico del Comune di Roma, vi introduce malware in modo tale da compromettere il funzionamento dello stesso sistema ed ottenere un finanziamento in assenza degli opportuni requisiti. 7) La Funzione interessata di Fondazione Bioparco di Roma, a fronte della necessità di dotare la Fondazione di una banca dati, anziché provvedere all'acquisto della licenza realizza un duplicato su un supporto "pirata" che viene detenuto presso gli uffici del l'ente. 8) La Funzione interessata di Fondazione Bioparco di Roma, a fronte della necessità di dotare alcuni terminali della Fondazione di un software commerciale, anziché provvedere all'acquisto della licenza realizza un duplicato su un supporto "pirata" attraverso cui provvede alla successiva installazione.
Attività di controllo: 1) Tracciamento di tutte le comunicazioni della Fondazione. 2) Devono essere previste riunioni periodiche tra il Direttore generale e l'Organismo di vigilanza per verificare l'attuazione delle regole di gestione. 3) Deve essere garantita la chiara definizione dei dati e delle informazioni che devono essere forniti al Direttore generale da parte dei Responsabili di ogni singola funzione aziendale. 4) Mantenere un efficace sistema di sicurezza informatica, in particolare attraverso la protezione dei sistemi e delle informazioni dai potenziali attacchi, attraverso l'utilizzo di strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attacchi, nonché la garanzia della massima continuità del servizio. 5) Assegnazione e gestione delle credenziali di autorizzazione personale (*username* e *password*) e delle credenziali di accesso alle diverse sezioni del sistema informatico della Fondazione. 6) L'accesso alle diverse sezioni del sistema informatico della Fondazione e a eventuali dati, informazioni, sistemi informatici e telematici cui la Fondazione abbia accesso è riconosciuto a

dipendenti, collaboratori, consulenti e *partner* nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico e coerentemente con gli obiettivi aziendali. 7) Ogni singolo utente è personalmente responsabile riguardo all'utilizzo del sistema informatico della Fondazione, inclusi eventuali dati, informazioni, sistemi informatici e telematici cui la Fondazione abbia accesso, nell'ambito dei presidi posti dalla Fondazione a tutela della sicurezza, integrità e riservatezza dei dati. 8) Divieto per amministratori, dipendenti, collaboratori, consulenti e partner, che a vario titolo abbiano accesso alla rete aziendale, di installare propri software che non rientrino nello scopo per cui il sistema informatico è stato assegnato all'utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale. 9) Divieto per amministratori, dipendenti, collaboratori, consulenti e partner di operare in maniera illecita su sistemi informativi altrui al fine di sottrarre fraudolentemente dati o informazioni riservate o sensibili. 10) L'installazione di nuove apparecchiature IT, strutture e procedure deve essere formalmente approvata dal Responsabile d'area, dovendo peraltro l'approvazione includere il parere favorevole del Responsabile della sicurezza Informatica. 11) Il processo di definizione ed approvazione di nuove strutture IT, e della loro modifica, deve essere sempre formalizzato; il processo di approvazione comprende un'analisi, effettuata dal settore aziendale sulla sicurezza informatica, avente come finalità quella di assicurare che le nuove tecnologie non presentino lacune sotto il profilo della sicurezza e non influenzino negativamente i sistemi e le procedure attualmente presenti. 12) Divieto per amministratori, dipendenti, collaboratori, consulenti e partner, che a vario titolo abbiano accesso alla rete aziendale, di installare nella rete propri software che possano impedire o interrompere o danneggiare le comunicazioni informatiche aziendali ovvero l'intero sistema informatico aziendale. 13) Costante interlocuzione tra i Responsabili d'area e l'OdV.

Fattore qualificante il controllo:

- Modello organizzativo;
- Codice etico;
- Istruzioni operative: v. *supra* § 4;
- Flussi informativi verso l'Organismo di Vigilanza.

6. Istruzioni e verifiche dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza in relazione al pericolo di commissione di reati informatici sono i seguenti:

i. monitoraggio dell'efficacia delle procedure aziendali qui positivizzate;

ii. esame di eventuali segnalazioni provenienti da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

7. Appendice: quadro sinottico dell'impatto dei reati informatici sulle prescrizioni in materia di *privacy* con riferimento alla sicurezza informatica

Codice penale	**Reati informatici previsti dal presente MOGC 231**	**GDPR**	**Principali violazioni/inadempimenti collegati ai reati informatici previsti dal MOGC 231**	
Art. 491-*bis*	Falsità riguardanti un documento informatico	• Art. 5 • Art. 6 • Art. 24 • Art. 25	• Dati trattati in modo lecito, corretto e trasparente • Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	Art. 4 c. 85 – violazione dati personali
		Art. 32	Sicurezza del trattamento	
Art. 615-*ter*	Accesso abusivo ad un sistema	• Art. 5 • Art. 6 • Art. 24	• Dati trattati in modo lecito, corretto e trasparente	Art. 4 c. 85 – violazione dati personali

	informatico o telematico	Art. 25	• Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	
		Art. 32	Sicurezza del trattamento	
Art. 615-*quater*	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici	• Art. 5 • Art. 6 • Art. 24 • Art. 25	• Dati trattati in modo lecito, corretto e trasparente • Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	Art. 4 c. 85 – violazione dati personali
		Art. 32	Sicurezza del trattamento	
Art. 615-*quinquies*	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	• Art. 5 • Art. 6 • Art. 24 • Art. 25	• Dati trattati in modo lecito, corretto e trasparente • Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	Art. 4 c. 85 – violazione dati personali
		Art. 32	Sicurezza del trattamento	
Art. 617-*quater*	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	• Art. 5 • Art. 6 • Art. 24 • Art. 25	• Dati trattati in modo lecito, corretto e trasparente • Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	Art. 4 c. 85 – violazione dati personali
		Art. 32	Sicurezza del trattamento	
Art. 617-*quinquies*	Installazione di apparecchiature atte ad intercettare,	• Art. 5 • Art. 6 • Art. 24	• Dati trattati in modo lecito, corretto e trasparente	Art. 4 c. 85 – violazione dati personali

	impedire o interrompere comunicazioni informatiche o telematiche	• Art. 25	• Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	
		Art. 32	Sicurezza del trattamento	
Art. 635-*bis*	Danneggiamento di informazioni, dati e programmi informatici	• Art. 5 • Art. 6 • Art. 24 • Art. 25	• Dati trattati in modo lecito, corretto e trasparente • Liceità del trattamento • responsabilità del titolare del trattamento • protezione dei dati fin dalla progettazione e per impostazione predefinita	Art. 4 c. 85 – violazione dati personali
		Art. 32	Sicurezza del trattamento	