

Allegato 4 al Modello Organizzativo ex D.Lgs. 231/01

REATI INFORMATICI

A. Premessa

I reati informatici sono previsti e disciplinati dagli artt. 24, e 24 bis D. Lgs. 231/01.

La tipologia di tali reati è caratterizzata da una maggiore difficoltà di accertamento rispetto agli altri reati di cui al D. Lgs. 231/01, in quanto, in linea teorica, i reati ivi previsti possono essere commessi da chiunque abbia accesso al sistema, indipendentemente dalla mansione svolta. Altro problema caratterizzante questa categoria di reati è dato dal fatto che non esistono delle aree o funzioni maggiormente a rischio, il che comporta la necessità di un'attenta vigilanza "trasversale" e di rigide procedure di controllo tali da scongiurarne la commissione. Le regole di comportamento ed i relativi controlli, per i motivi su esposti, dovranno pertanto investire tutti i dipendenti e finanche i fornitori esterni cui vengono commissionati specifici servizi in materia, tali da poter esporre l'Ente a sanzioni rilevanti ex D. Lgs. 231/2001.

Altro aspetto peculiare delle fattispecie in esame è che le stesse, nella maggior parte dei casi, sono strumentali rispetto al raggiungimento di uno scopo ulteriore tale da palesare il reato solo a seguito del raggiungimento dello scopo previsto, il che rende ulteriormente difficile l'accertamento a priori in assenza di un adeguato ed efficace modello organizzativo.

In considerazione di quanto esposto è assolutamente necessario, per scongiurare la responsabilità penale della Società ed assicurare alla stessa la scriminante prevista dal D. Lgs. 231/01, predisporre, adottare ed efficacemente attuare la sorveglianza ed il controllo di cui al presente documento.

I reati informatici possono essere commessi da qualsiasi operatore in ambito aziendale, a prescindere dall'area di appartenenza.

Nel documento di analisi dei rischi, si è teso pertanto a valutare la possibile commissione proiettando le procedure atte alla prevenzione, tenendo conto della trasversalità delle condotte pur cercando, laddove possibile, di circoscrivere le aree di interesse.

Si esamini, prima di tutto, il testo delle disposizioni richiamate, riportati integralmente di seguito.

A tale riguardo si rappresenta che l'art. 24 del D. Lgs.231/2001, tra le altre fattispecie previste, contempla anche quella della frode informatica a danno dello Stato o di altro Ente Pubblico, motivo per cui si riporta la specifica previsione.

B. Tipologie di reato

Art. 24 D. Lgs.231/01

“OMISSIS...Frode informatica in danno dello Stato o di un ente pubblico”

In relazione alla commissione dei delitti di cui.....OMISSIS.... all'art.640-ter (Frode informatica) se commesso a danno dello Stato o di altro ente pubblico.....OMISSIS...si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità si applica la sanzione pecuniaria da duecento a seicento quote.

2-bis. Si applicano all'ente le sanzioni previste ai commi precedenti in relazione alla commissione del delitto di cui all'articolo 2 della legge 23 dicembre 1986, n. 898.

Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9 comma 2, lettere c), d) ed e).

Art. 24 bis D. Lgs. 231/01:

“Delitti informatici e trattamento illecito di dati”

1. *In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da duecento a settecento quote.*

1-bis. *In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.*

2. *In relazione alla commissione dei delitti di cui agli articoli 615-quater e 635-quater.1 del codice penale, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*

3. *In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*

4. *Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per il delitto indicato nel comma 1-bis si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni. Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).*

Art. 25-sexies D. Lgs. 231/01:*“Abusi di mercato”*

1. *In relazione ai reati di abuso di informazioni privilegiate e di manipolazione del mercato previsti dalla parte V, titolo I-bis, capo II, del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, si applica all'ente la sanzione pecuniaria da quattrocento a mille quote.*
2. *Se, in seguito alla commissione dei reati di cui al comma 1, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.*

Art. 25 octies.1 D. Lgs. 231/01:*“Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori”*

1. *In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:*
 - a. *Per il delitto di cui all'articolo 493-ter, la sanzione pecuniaria da trecento a ottocento quote;*
 - b. *Per il delitto di cui all'articolo 493-quater e per il delitto di cui all'articolo 640-ter nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria sino a cinquecento quote.*
2. *Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:*
 - a. *se il delitto è punito con la pena della reclusione inferiore a dieci anni, la sanzione pecuniaria sino a cinquecento quote;*
 - b. *se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da trecento a ottocento quote.*
- 2-bis. *In relazione alla commissione del delitto di cui all'art. 512-bis del codice penale, si applica all'ente la sanzione pecuniaria da 250 a 600 quote.*
3. *Nei casi di condanna per uno dei delitti di cui ai commi 1, 2 e 2-bis si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2*

Art. 25 novies D. Lgs. 231/01:

“Delitti in materia di violazione del diritto d'autore”

- 1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.*
- 2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941.*

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

Modalità di commissione del reato:

L'intrusione abusiva in un sistema informatico o telematico si concretizza non appena vengono superate le misure di sicurezza del sistema stesso, siano esse di tipo logico ma anche strumenti di tipo organizzativo in quanto destinati a regolare l'ingresso ai locali in cui gli impianti sono custoditi. È punita la semplice intrusione senza alcuna differenza in seno all'effettivo danneggiamento o furto dei dati.

Possono commettere il delitto di cui all'art. 615 ter c.p. anche soggetti che si mantengano in un sistema contro la volontà espressa o tacita di chi abbia il diritto di escluderli.

La norma prevede poi un inasprimento di pena nel caso in cui:

1. il fatto sia 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 eserciti anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2. il colpevole per commettere il fatto usi minaccia o violenza sulle cose o alle persone, ovvero sia palesemente armato;
3. dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati, delle informazioni o dei programmi in esso contenuti.

Inoltre, qualora i fatti 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 ulteriormente aumentata.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

Il reato di accesso abusivo può far riferimento ad accessi a sistemi interni o esterni configurandosi a seconda dell'obiettivo del reato.

In merito all'accesso al sistema interno, sono particolarmente sensibili le aree inerenti la gestione amministrativa (in relazione ai dati di bilancio, fatturazione, ecc.), le attività di delivery in particolare per quanto concerne l'accesso ai dati di registrazione utenza, di navigazione e relative alla posta elettronica.

Per quanto riguarda, invece, l'**eventuale accesso a sistemi esterni** (ad es. sistemi informatici di clienti di GFT), l'area sensibile è rappresentata dalla gestione delle attività di delivery, che è a contatto con i clienti.

Occorre, comunque, concludere rappresentando come possano comunque ritenersi estesi i rischi di accesso abusivo, trasversalmente a tutte le aree coperte dalla gestione dei sistemi informativi in considerazione del frazionamento delle informazioni e dei dati di cui è titolare l'azienda.

I principali controlli implementati da GFT per **prevenire accessi abusivi al sistema interno** sono quelli che riguardano i processi di: creazione, modifica e cancellazione di account e di profili, l'utilizzo di sistemi di crittografia, gestione reti interne, implementazione e manutenzione, accettabile utilizzo degli asset e sicurezza e manutenzione dei sistemi.

Per quanto riguarda l'eventuale **accesso abusivo ai sistemi di terzi** (ad esempio dei clienti) i controlli implementati riguardano i processi di: collegamento dalla rete GFT alla rete del cliente e sviluppo sicuro di Software. Al riguardo si evidenzia che le attività di sviluppo vengono eseguite su appositi ambienti di test dove confluiscono dati che si trovano nei programmi di produzione dei clienti, ma che tramite software specifici sono anonimizzati o mascherati. Nello svolgimento dell'attività di sviluppo software, quindi, solitamente i dipendenti di GFT non hanno accesso diretto ai sistemi di produzione del cliente e comunque ogni eventuale accesso risulta tracciato tramite sistemi di log. Inoltre, GFT promuove iniziative sulla formazione e selezione dei propri dipendenti, nonché sui controlli di qualità di prodotto.

Intercettazione, Impedimento o Interruzione Illecita di Comunicazioni Informatiche o Telematiche (art. 617-quater c.p.) – Detenzione, Diffusione e Installazione Abusiva di Apparecchiature e di Altri Mezzi per Intercettare, Impedire o Interrompere Comunicazioni Informatiche (art. 617-quinquies c.p.)

Modalità di commissione del reato:

L'**art. 617-quater** sanziona l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche o intercorrenti tra più sistemi (comma 1), nonché la condotta di chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni sopra indicate (comma 2).

In ordine alla condotta occorre precisare che l'intercettazione deve essere caratterizzata da una modalità fraudolenta, compendosi con strumenti idonei a celarla ai comunicanti e/o al sistema

informatico programmato per negare automaticamente gli accessi e le abusive intromissioni nelle comunicazioni informatiche e/o telematiche.

La Legge 90/2024 ha modificato il comma 4 prevedendo la procedibilità d'ufficio, a differenza dei commi 1 e 2 dove la punibilità richiede la querela della persona offesa, se il fatto è commesso: 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma; 2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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.

L'art. 617-quinquies punisce chiunque, al fine di intercettare, impedire o interrompere la comunicazione relative a uno o più sistemi informatici, si procura, produce, riproduce, diffonde, importa, comunica, consegna, mette in qualunque modo a disposizione di terzi ovvero installa apparecchiature o altri strumenti atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

La Legge 90/2024 ha introdotto i commi 2 e 3 prevedendo due ipotesi aggravate, quando: i) ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2; ii) ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1.

Ciò che si intende tutelare con gli articoli 617-quater e 617-quinquies, sono la libertà e la riservatezza delle comunicazioni informatiche, al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi, a prescindere, quindi, dal documento arrecato.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

Anche in questo caso i reati possono essere commessi sia in riferimento a sistemi interni o esterni.

I principali controlli implementati da GFT per prevenire l'intercettazione, la diffusione, l'impedimento o l'interruzione illecita di comunicazioni nel sistema interno sono quelli che riguardano i processi di: creazione, modifica e cancellazione di account e di profili, utilizzo di sistemi di crittografia, gestione reti interne, implementazione e manutenzione, accettabile utilizzo degli asset e sicurezza e manutenzione dei sistemi.

Per quanto riguarda l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni su sistemi di terzi (ad esempio dei clienti) i controlli implementati riguardano i processi di: collegamento dalla rete GFT alla rete del cliente e sviluppo sicuro di Software. Con particolare riferimento a tali fattispecie di reato si evidenzia che all'esito dello sviluppo di un prodotto, quest'ultimo prima di essere utilizzato dal cliente viene sottoposto a vari livelli di controllo: controllo di GFT su ogni singola unità sviluppata (Unit Test), controllo di secondo livello del cliente c.d. system integration test (che coinvolge tutte le componenti del software), ultima fase di controllo detta User Acceptance test, gestita dal business del Cliente. Pertanto, eventuali installazioni di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico sarebbero senz'altro rilevate.

Danneggiamento di Informazioni, Dati e Programmi Informatici (art. 635-bis c.p.) – Danneggiamento di Informazioni, Dati e Programmi Informatici pubblici o di interesse pubblico (art. 635-ter c.p.) – Danneggiamento di Sistemi Informatici o Telematici (art.635-quater c.p.) – Danneggiamento di Sistemi Informatici di Pubblico Interesse (art. 635-quinquies c.p.)

Modalità di commissione del reato:

Gli articoli 635-bis e 635-ter c.p., sanzionano i fatti di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui, privati e pubblici.

Gli articoli 635-quater e 635-quinquies c.p., proteggono invece da analoghe condotte di danneggiamento i sistemi informatici o telematici, privati e pubblici.

Con riferimento agli artt. 635-bis e 635-quater c.p., la Legge 90/2024 ha introdotto in entrambe le fattispecie il comma 2 prevedendo due ipotesi aggravate quando: i) 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) il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

Anche con riferimento agli artt. 635-ter e 635-quinquies c.p., la Legge 90/2024 ha introdotto, in entrambe le fattispecie, i commi 2 e 3 prevedendo delle ipotesi aggravate quando: 1) 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) il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato; 3) dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici; 4) taluna delle circostanze di cui ai numeri 1) e 2) concorre con taluna delle circostanze di cui al numero 3).

Oggetto di danneggiamento può essere innanzitutto il sistema informatico, eventualmente collegato a distanza con altri elaboratori, come nel caso dei sistemi telematici, e l'aggressione può riguardare tanto il sistema nel suo complesso quanto una o più delle sue componenti materiali, nonché i dati e i programmi informatici e le informazioni contenute nel sistema. Sulla base del dato testuale si deve ritenere che l'espressione sistema informatico contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzo (anche di parte) di tecnologie informatiche.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

Tali reati possono essere commessi su dati, programmi e informazioni presenti su sistemi interni o su sistemi di terzi (ad esempio clienti o concorrenti).

I principali controlli implementati da GFT per prevenire danneggiamenti di dati, informazioni e programmi interni sono quelli che riguardano i processi di: creazione, modifica e cancellazione di account e di profili, utilizzo di sistemi di crittografia, gestione reti interne, implementazione e manutenzione, accettabile utilizzo degli asset e sicurezza e manutenzione dei sistemi.

Per quanto riguarda l'eventuale danneggiamento su sistemi di terzi (ad esempio dei clienti e concorrenti) i controlli implementati riguardano i processi di: collegamento dalla rete GFT alla rete del cliente e sviluppo sicuro di Software. Al riguardo, si evidenzia che le attività eventualmente svolte su sistemi dei clienti sono registrate mediante sistemi di registrazione di Log. Inoltre, sono previste particolari regole che riguardano i casi di sospetto incidente di sicurezza informatico sia interno sia sui sistemi dei clienti.

Detenzione, Diffusione e Installazione Abusiva di Apparecchiature, Codici e Altri Mezzi Atti all'Accesso a Sistemi Informatici o Telematici (art. 615-quater c.p.)

Modalità di commissione del reato:

Il reato di cui **all'art. 615-quater c.p.** sanziona la condotta di chi, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, **abusivamente** si procura, detiene, produce, riproduce, diffonde, importa, comunica o consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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.

La Legge 90/2024 ha introdotto i commi 2 e 3 prevedendo due ipotesi aggravate quando: i) 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; ii) i fatti 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.

Il bene giuridico tutelato dalla norma in esame è in primis la tutela anticipata del domicilio informatico e la segretezza dei dati e dei programmi contenuti in un elaboratore. In un'accezione più ampia, invece, la fattispecie attribuisce una funzione di tutela più estesa ed anticipata rispetto ai beni quali il patrimonio, la riservatezza e la fede pubblica. Si sostanzia, quindi, come una norma preordinata a prevenire, anche, la realizzazione di illeciti informatici.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

GFT ha adottato numerose procedure atte a regolare la gestione dei codici di accesso a sistemi informatici ed in particolare ha regolamentato i processi di creazione, modifica e cancellazione di account e di profili, nonché di limitazione di accesso e strumenti di autenticazione.

Detenzione, Diffusione e Installazione Abusiva di Apparecchiature, Dispositivi o Programmi Informatici Diretti a Danneggiare o Interrompere un Sistema Informatico o Telematico (art. 635-quater.1 C.P.)**Modalità di commissione del reato:**

Il reato di cui all'art. 635-quater.1 c.p. sanziona la condotta di chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

Ai sensi del secondo e del terzo comma, la pena è aggravata quando ricorra una delle circostanze di cui all'art. 615-ter c.p. ovvero quando il fatto riguarda i sistemi informatici o telematici di cui al terzo comma dell'art. 615-ter c.p.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

Tale reato potrebbe configurarsi maggiormente nelle attività eseguite dal delivery relativamente alla fase di sviluppo e successiva diffusione di software. Con particolare riferimento a tale fattispecie di reato si evidenzia che all'esito dello sviluppo di un prodotto, quest'ultimo prima di essere venduto e utilizzato dal cliente viene sottoposto a vari livelli di controllo: controllo di GFT su ogni singola unità sviluppata (Unit Test), controllo di secondo livello del cliente c.d. system integration test (che coinvolge tutte le componenti del software), ultima fase di controllo detta User Acceptance test, gestita dal business del Cliente. Pertanto, eventuali installazioni di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico sarebbero senz'altro rilevate.

Falsità di Documenti Informatici (art. 491-bis c.p.)**Modalità di commissione del reato:**

La fattispecie di cui trattasi estende ai documenti informatici pubblici aventi efficacia probatoria la medesima disciplina prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del Codice Penale (non sembrano trovare applicazione le norme che sanzionano la falsità di fogli firmati in bianco, artt. 486, 487, 488 c.p.) in particolare ci si riferisce ai reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri o notificazioni, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

L'oggetto della falsificazione, prima rappresentato sia da documenti privati sia da documenti pubblici, è stato limitato per effetto del D. Lgs. n. 7/2016 al solo documento informatico pubblico.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

La predisposizione e l'utilizzazione di atti falsi si concretizza in una falsificazione a carattere virtuale, cioè una "simulazione" di un dato in realtà inesistente o "composto" da parti (grafiche o fotografiche) vere tagliate e incollate per finalità fraudolente, o falsamente attestanti un evento o una sottoscrizione nel caso, in verità più sofisticato, della alterazione dei dati alfanumerici che compongono le forme di sottoscrizione e di validazione degli atti pubblici e privati emessi o immessi in rete.

La portata applicativa della norma è estesa e può investire i più ampi settori societari, ma considerata la complessità della fattispecie deve riferirsi, principalmente, agli organi direttivi ed al complesso decisionale – manageriale quale possibile utilizzatore del documento stesso all'interno della compagine societaria o parti di essa ovvero nei confronti di altre società o parti di essa.

Le aree di particolare interesse sono l'amministrazione, l'Area Operation nonché l'area in cui si svolgono attività presso ufficio acquisti, l'ufficio competente per la gestione gare o con competenze rispetto alla sicurezza sui luoghi di lavoro ed agli aspetti inerenti la gestione ambientale. A livello più generale tutte le aree nelle quali sono possibili accessi (fisici e non) al Sistema Informatico, comprese le banche dati, le postazioni di lavoro, i server interni ed i server esterni dove sono allocati dati dell'Ente.

Frode Informatica del Soggetto che Presta Servizi di Certificazione di Firma Elettronica (art. 640-quinquies c.p.)

Modalità di commissione del reato:

Il reato punisce il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

I certificatori accreditati sono soggetti pubblici o privati che emettono certificati qualificati conformi alla Direttiva europea 1999/93/CE ed alla normativa nazionale in materia.

L'azienda non è soggetto accreditato quale certificatore e pertanto non può, fatto salvo il concorso, commettere, da sola o direttamente, l'illecito in questione. Affinché l'Azienda sia chiamata a rispondere del reato in questione è necessario che vi sia un concorso della stessa con un soggetto certificatore accreditato.

La rischiosità, intesa nel senso di probabilità di verifica di illeciti fondanti una responsabilità ex D. Lgs. 231/2001 per l'Azienda, si situa a livello di rapporti tra la società e i certificatori accreditati.

Estorsione (Art. 629, comma 3 c.p.)

Modalità di commissione del reato:

Il reato punisce chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

La pena è aggravata nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità nonché se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628, pertanto: 1) se la violenza o minaccia è commessa con armi o da persona travisata, o da più persona riunite; 2) se la violenza consiste nel porre taluno in stato di incapacità di volere o di agire; 3) se la violenza o minaccia è posta in essere da persona che fa parte dell'associazione di cui all'art. 416-bis; 3-bis) se il fatto è commesso nei luoghi di cui all'art. 624-bis o in luoghi tali da ostacolare la pubblica o privata difesa; 3-ter) se il fatto è commesso all'interno di mezzi di pubblico trasporto; 3-quater) se il fatto è commesso nei confronti di persona che si trovi nell'atto di fruire ovvero che abbia appena fruito dei servizi di istituti di credito, uffici postali o sportelli automatici adibiti al prelievo di denaro; 3-quinquies) se il fatto è commesso nei confronti di persona ultrasessantacinquenne.

Valgono pertanto tutte le considerazioni già espresse con riferimento agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies a cui si aggiunge il dolo generico di costringere il soggetto passivo a fare o ad omettere qualche cosa conseguendo un ingiusto profitto con altrui danno.

Per i soggetti attivi ed i presidi di controllo implementati da GFT si rimanda alle modalità commissive delle singole fattispecie.

Frode Informatica (art. 640-ter c.p.)

Modalità di commissione del reato:

Il reato di frode informatica ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa, dalla quale si distingue solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

La frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui, dovendosi all'uopo precisare che mentre il requisito del profitto ingiusto può comprendere in sé qualsiasi utilità, incremento o vantaggio patrimoniale, anche a carattere non strettamente economico, l'elemento del danno deve avere necessariamente contenuto patrimoniale.

I soggetti attivi del reato potrebbero essere, quindi, tutti i dipendenti della Società che possono assumere i seguenti ruoli: utente assegnatario di profilo di autorizzazione e amministratore di sistema.

Le aree di particolare interesse sono: Area amministrativa, Area Operation, area competente per la partecipazione a gare, bandi, area acquisti. Tenzialmente sono da ritenersi sensibili e rischiose tutte le aree nelle quali è possibile un accesso (fisico e no) al Sistema Informatico, comprese le banche dati, le postazioni di lavoro, i server interni ed i server esterni dove sono allocati dati dell'Ente.

Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)

Modalità di commissione del reato:

La fattispecie punisce chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque ogni altro strumento di pagamento diverso dai contanti.

Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali carte tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)

Modalità di commissione del reato:

Salvo che il fatto costituisca più grave reato, la fattispecie punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

I soggetti attivi di entrambe le fattispecie potrebbero essere, quindi, tutti i dipendenti della Società che creino apparecchiature, dispositivi o programmi informatici diretti a realizzare le condotte descritte, ovvero in occasione di un qualsiasi pagamento che venga effettuato con metodi di pagamenti diversi dai contanti.

Le aree di particolare interesse sono: Area amministrativa, Area Operation, area acquisti. Tenzialmente sono da ritenersi sensibili e rischiose tutte le aree nelle quali è possibile effettuare un pagamento ovvero predisporre un sistema per i clienti per effettuare i pagamenti.

Legge sulla protezione del diritto d'autore (art. 171-bis, modificato dalla L. 166/2024)**Modalità di commissione del reato:**

La fattispecie punisce 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 ai sensi della presente legge.

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. Viene altresì prevista una cornice minima edittale se il fatto è di rilevante gravità.

La medesima fattispecie, poi, al secondo comma, punisce chiunque, al fine di trarne profitto, su supporti non contrassegnati ai sensi della presente legge 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. Anche per tali condotte viene prevista una cornice minima edittale se il fatto è di rilevante gravità.

Legge sulla protezione del diritto d'autore (art. 171-ter, modificato dalla L. 166/2024)**Modalità di commissione del reato:**

Se il fatto è commesso per uso non personale, la fattispecie punisce la condotta di chi: a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b); d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze

di immagini in movimento, od altro supporto per il quale è prescritta l'apposizione di contrassegno ai sensi della presente legge, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato; f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto; f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'articolo 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure; h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; h-bis) abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovisivo, 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.

La medesima fattispecie, punisce altresì chiunque: a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante concessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa; b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1; c) promuove o organizza le attività illecite di cui al comma 1.

Manipolazione del mercato (art. 185 D. Lgs. n. 58/1998, modificato dalla L. 132/2025)

Modalità di commissione del reato:

La fattispecie punisce chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari e prevede una cornice edittale specifica per l'ipotesi in cui il fatto sia commesso mediante l'impiego di sistemi di intelligenza artificiale.

Viene poi individuata una causa di non punibilità per chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del regolamento (UE) n. 596/2014.1569

Da ultimo, è previsto che il giudice possa aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

C. Principi generali di Comportamento

Al fine di prevenire i reati informatici rilevanti ai fini 231, oltre alle procedure di seguito indicate, ciascun utente è tenuto a rispettare i seguenti principi di comportamento e nello specifico **è obbligo dell'utente informatico:**

- **astenersi** da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui;
- **astenersi** dal compiere azioni e/o condotte che possano permettere l'acquisizione colposa o dolosa da parte di terzi di un codice identificativo, di un diritto di accesso, password e di qualsiasi altra credenziale ad esso assegnata;
- **attuare i comportamenti** richiesti dalla Società e necessari per proteggere il sistema informativo, ivi inclusi gli specifici divieti di installazione di software in autonomia;

in caso di utilizzo di sistemi di intelligenza artificiale **attenersi ai seguenti principi**: i) garantire la trasparenza nei sistemi di intelligenza artificiale. Spiegare come vengono prese le decisioni dall'algoritmo; ii) sviluppare sistemi di intelligenza artificiale imparziali. Verificare regolarmente eventuali risultati discriminatori; iii) condurre test di sicurezza e valutazione del rischio. Affrontare i potenziali danni; iv) mantenere la revisione umana sulle decisioni critiche in materia di intelligenza artificiale; v) collaborare a livello globale per stabilire standard comuni per l'intelligenza artificiale; vi) informare utenti sulle capacità e i limiti dell'IA nonché promuovere consapevolezza.

Sono invece **vietate**, tra le altre, le seguenti condotte:

- comunicare le credenziali di accesso a qualsiasi soggetto esterno;
- diffondere le informazioni societarie inerenti l'uso dei mezzi informatici aziendali e l'accesso a dati, sistemi e applicazioni aziendali;
- utilizzare la rete ai fini di operazioni di remote banking personali e/o comunque non attinenti l'Azienda o l'attività e le mansioni cui l'utente è preposto;

- installare ed utilizzare apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale;
- installare sul pc aziendale, sui server e su ogni supporto removibile, programmi atti a rimuovere o eludere i dispositivi di protezione di software per elaboratori;
- riprodurre o trasferire su altro supporto, il contenuto di una banca dati, salvo che ciò sia in adempimento alle necessità aziendali e previa verifica con il Dirigente competente;
- vendere o concedere in locazione banche di dati aziendali;
- connettere i server interni e le postazioni di lavoro a dispositivi astrattamente idonei ad essere connessi alla rete esterna ed a inviare o ricevere dati dall'esterno;
- connettere i server interni e le postazioni di lavoro a dispositivi di memorizzazione di massa o altri supporti magnetici, salvo specifiche esigenze degli amministratori della Struttura IT;
- utilizzare tecnologie di trasferimento dati senza connessione fisica (es. wireless), o tramite altra tecnologia di trasferimento dati in ingresso o in uscita, dai server interni e dalle postazioni di lavoro;
- installare, utilizzare o distribuire software commerciali senza aver preventivamente ottenuto le necessarie licenze d'uso e le relative autorizzazioni secondo il processo aziendale;
- utilizzare software con licenze scadute, sospese o revocate, ovvero eccedere i limiti di utilizzo previsti dai termini contrattuali delle licenze acquisite;
- acquisire, installare o utilizzare software ottenuti tramite canali non ufficiali, inclusi software modificati o distribuiti in violazione dei diritti di proprietà intellettuale dei legittimi titolari;
- prelevare dalla rete documenti, files o dati non attinenti lo svolgimento delle attività aziendali relative alle mansioni ed ai progetti in cui l'utente opera;
- utilizzare programmi idonei a modificare o alterare un documento salvo necessità aziendali per le quali deve essere prevista un'apposita autorizzazione espressa;
- effettuare installazioni di meccanismi di distribuzione di applicazioni e pacchetti alternativi a quelli ufficialmente forniti dall'Azienda, modificare il firmware od adottare procedure di sblocco a vario titolo sullo strumento di telefonia mobile messo a disposizione;
- gestire in modo non corretto i rapporti con certificatori accreditati;
- porre in essere qualsiasi condotta finalizzata alla violazione, da parte dei soggetti certificatori accreditati, degli obblighi di legge per il rilascio di certificati qualificati;
- utilizzare sistemi di intelligenza artificiale per elaborare, analizzare o processare dati personali, informazioni riservate o dati dei clienti tramite piattaforme pubbliche o non autorizzate dalla Società;

- utilizzare output generati da sistemi di intelligenza artificiale in processi decisionali critici o in comunicazioni ufficiali senza preventiva revisione e validazione umana;
- bypassare o disattivare i controlli di sicurezza, i filtri di contenuto o le limitazioni d'uso implementati sui sistemi di intelligenza artificiale autorizzati dalla Società.

D. Esistenza di procedure, linee guida e prassi operative consolidate:

Codice Etico; Policy di Sicurezza Informatica e Standard per le utenze; Clausole Contrattuali; Documentazione ed attività tecniche funzionali all'applicazione del Provvedimento in materia di Amministratore di Sistema; Procedure, Istruzioni operative, Istruzioni di lavoro; 900 FRM Richiesta strumenti aziendali; Policy del Gruppo GFT: Access Control Policy, Acceptable use of Assets Policy, Asset Management Policy, Information Security Awareness and Training Policy, Backup Policy, Business Continuity and Crisis Management Policy, Change Management Policy, Cryptography Policy, Secure Disposal and Re-Use Policy, Human Resources Security Policy, Information Security Incident Management Policy, Information Classification Policy, ISMS Policy, Labelling Policy, Malware Protection Policy, Mobile Policy, Network Policy, Password Policy, Physical Security Policy, Secure Development Policy, Information Security Teleworking Policy, Third parties Information Security Policy, Cloud Policy, Forensics Policy, Remote Client Access Security. .

E. Regolamentazione dei processi connessi ai reati informatici e segregazione dei compiti

a) Creazione, modifica e cancellazione di account e di profili

L'account viene creato dall'IT al momento dell'ingresso del soggetto in Azienda, previa comunicazione da parte dell'ufficio del personale per la definizione delle banche dati accessibili, necessarie per l'adempimento delle mansioni richieste.

In capo all'ufficio People sussiste il dovere di tempestiva segnalazione all'IT

in merito ad eventuali cambi di mansioni e/o interruzioni del rapporto di lavoro dei dipendenti/collaboratori. In conseguenza di ciò l'IT predispone le modifiche del caso ai profili di accesso ed autorizzazione degli utenti.

In capo all'IT sono imposti dei doveri di monitoraggio in merito ai profili di autorizzazione degli utenti.

Limitazione di accesso e strumenti di autenticazione

L'IT verifica periodicamente che gli accessi degli utenti informatici alle informazioni che risiedono sui server e sulle banche dati aziendali siano conformi alle loro credenziali di autorizzazione.

Sono previste speciali credenziali di autenticazione per gli amministratori di sistema e per gli addetti alla manutenzione.

E' previsto un sistema di autorizzazione per l'accesso alle applicazioni.

La rete di trasmissione dati aziendale viene costantemente protetta da adeguati strumenti di limitazione degli accessi (firewall e proxy) sempre attivi ed aggiornati al fine di prevenire qualsiasi condotta atta a danneggiare o interrompere il sistema dall'interno o dall'esterno.

I dispositivi telematici di instradamento sono collocati in aree dedicate e protette e sono accessibili solo al personale espressamente autorizzato.

I dettagli dei controlli relativi a tali processi sono contenuti nella Access Control Policy e nella Password Policy.

b) Utilizzo di sistemi di crittografia

I controlli di crittografia sono necessari per tutti i dispositivi come computer portatili, workstation o dispositivi mobili utilizzati per memorizzare o accedere a dati aziendali non pubblici in aree non sicure.

Ogni documento di proprietà di GFT è classificato sulla base della Information Classification Policy, che individua le modalità di trasmissione delle informazioni e dell'utilizzo di sistemi di crittografia sulla base della loro classificazione (pubblica, ristretta o confidenziale). Inoltre, a prescindere dalla loro classificazione e salvo che siano considerati ad uso esclusivamente interno, i documenti di proprietà di GFT, quando necessario, possono essere condivisi in presenza di autorizzazione scritta con parti esterne interessate, quali clienti, fornitori o altri terzi.

I dettagli dei controlli relativi al processo sono contenuti nella Cryptography Policy.

c) Gestione reti interne, implementazione e manutenzione

La rete interna è istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa e non può essere utilizzata per scopi diversi da quelli ai quali è destinata, senza espressa autorizzazione scritta di IT.

È fatto divieto di far circolare nella rete interna file non espressamente autorizzati, né software non forniti da GFT né alcuna altra notizia, informazione o dato non inerente l'attività aziendale.

Solo i dispositivi di GFT sono autorizzati a connettersi alla rete aziendale.

L'accesso alla rete interna GFT da parte di esterni è permessa solo previa approvazione da parte dell'Ufficio IT in casi eccezionali e comunque in questi casi l'accesso deve essere limitato nel tempo e sempre registrato.

Prima di consentire l'accesso alla rete GFT, l'utente esterno deve essere a conoscenza delle Policy e degli standard di sicurezza pertinenti alle proprie mansioni.

Agli utenti non è consentito trasferire o archiviare informazioni di GFT o dei clienti di GFT al di fuori dell'infrastruttura GFT senza previa approvazione scritta.

I dettagli dei controlli relativi al processo sono contenuti nella *Network Policy*.

d) Accettabile utilizzo degli asset

Corretto utilizzo strumenti informatici aziendali

Al momento della consegna della strumentazione informatica, l'utente riceve una mail con l'indicazione dell'asset assegnato, mentre in un software interno che gestisce inventari e assegnazioni (CMDV) vengono registrati gli asset fisici assegnati a ogni dipendente.

Gli strumenti informatici sono consegnati con la configurazione standard aziendale e ogni nuova ed ulteriore installazione potrà essere effettuata solo previa autorizzazione, a seguito di richiesta scritta (tramite trouble ticket), dell'IT. La richiesta deve attestare la preventiva valutazione di necessità dell'installazione.

Non è permesso aggirare le impostazioni di sistema fornite dall'IT del Gruppo GFT e le applicazioni di sicurezza per l'installazione di software aggiuntivi.

Se non si è certi sull'utilizzo dei software aggiuntivi, contattare l'IT del Gruppo GFT e richiederne il permesso.

È necessario utilizzare software in conformità con le condizioni ed i termini del Contratto di Licenza per gli stessi.

I software utilizzati su hardware del Gruppo GFT devono essere gratuiti o autorizzati dal Gruppo GFT. I Software non utilizzati devono essere disinstallati.

Relativamente alle attività di assistenza e manutenzione le stesse sono richieste tramite apposito ticket dall'Utente. In caso di allontanamento dalla postazione anche in via temporanea l'utente informatico attiva il sistema di protezione screen server, che consenta riavvio della schermata previa inserimento password.

È assolutamente vietato a tutti i dipendenti e collaboratori dell'Azienda rilasciare le credenziali di accesso a soggetti interni e/o esterni senza espressa autorizzazione della struttura IT. Nel caso la comunicazione si renda necessaria per interventi di natura tecnica, è fatto obbligo all'utente di provvedere immediatamente al cambio della password appena cessato l'intervento.

I dettagli dei controlli relativi al processo sono contenuti nella *Asset Management Policy* e nella *Acceptable use of Assets Policy*.

Corretto utilizzo posta elettronica

A tutti gli utenti viene assegnata una casella di posta elettronica al momento dell'ingresso in azienda.

A prescindere dal blocco tecnico sussistente, qualora si ricevano messaggi contenenti estensioni anomale, prima del download degli allegati ai messaggi di posta in entrata, il lavoratore deve accertare la provenienza dello stesso messaggio contenente file con estensione .exe, .bat, .xml, .vbs, .vb, .zip. In caso di dubbi, l'utente deve contattare IT.

È fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza degli obblighi di fedeltà e correttezza.

Corretta gestione rete internet

Sono assolutamente vietati ai dipendenti, ai collaboratori esterni ed ai fornitori l'accesso e la navigazione in siti non inerenti l'attività aziendale di qualsivoglia natura, poiché il collegamento ad Internet è esclusivamente finalizzato all'esercizio della stessa.

L'uso personale è consentito purché non consumi più di una quantità trascurabile di risorse di sistema, non interferisca con la produttività e non precluda alcuna attività aziendale.

Sono vietate la partecipazione, per motivi non professionali a mailing list, forum, community e le registrazioni, anche utilizzando pseudonimi (nicknames) in guest book e bacheche elettroniche chat o altri mezzi di comunicazione telematica non attinenti l'attività lavorativa, attuate mediante il pc aziendale.

Dismissione e smaltimento asset

La sanificazione di un supporto di memorizzazione elettronica da smaltire deve essere eseguita tramite cancellazione sicura (purgino) o distruzione, oppure tramite altre misure di salvaguardia (es. la cancellazione delle chiavi di cifratura), in modo da garantire che i dati non possano essere recuperati.

La sanificazione deve essere eseguita in tutti i casi, indipendentemente dagli altri controlli di sicurezza in vigore, ad esempio la crittografia del file system.

La sanificazione eseguita utilizzando la funzione di cancellazione di un sistema operativo non è una attività sufficiente da eseguire su un supporto di memorizzazione elettronica da smaltire.

I dettagli dei controlli relativi al processo sono contenuti nella Secure Disposal and Re-Use Policy.

e) Gestione Data base affidati a soggetti esterni

I fornitori di servizi informatici sono stati scelti previa valutazione delle caratteristiche di esperienza, capacità affidabilità e professionalità anche in merito all'adempimento di specifici servizi tecnici ad essi demandati da GFT.

GFT ha impegnato detti fornitori esterni mediante dettagliate clausole contrattuali o nomine a responsabili esterni del trattamento per garantire la sicurezza informatica dei sistemi e delle banche dati gestite esternamente dai medesimi fornitori.

Si chiarisce che detti fornitori sono pattiziamente obbligati ad assicurare ed a garantire a GFT un puntuale controllo sulle misure di sicurezza intraprese, siano esse fisiche/organizzative o logiche.

Ciascun fornitore è tenuto preventivamente ad aderire e ad adeguarsi alla policy aziendale in materia 231 ed alle clausole di riservatezza sussistenti in materia di protezione dati.

L'IT provvede alla verifica preliminare da parte delle attività di amministrazione di sistema di competenza del nuovo fornitore, provvedendo ad assegnare ad ogni nuovo operatore, apposito profilo sottoposto a loggatura ai sensi del provvedimento del Garante della privacy italiano in materia ADS del 2008.

I fornitori si impegnano a rispettare la *Third Parties Information Security Policy*.

f) Gestione backup e data base

I backup dei database sono disciplinati e regolamentati secondo la Backup Policy.

La manutenzione dei vari DB deve essere eseguita periodicamente secondo quanto definito dalla policy, salvo esigenze di natura estemporanea.

In caso di attività svolte in locale, è fatto obbligo all'utente informatico di seguire le linee guida fornite dall'IT in merito al salvataggio dei file nelle cartelle su cui è istituito il backup.

g) Gestione dei dispositivi mobili

I dispositivi di proprietà di GFT che appartengono al dominio (computer) sono gestiti, controllati e aggiornati dalla Società, mentre i telefoni mobili e i tablet di proprietà di GFT sono controllati tramite la piattaforma GFT MDM.

I dispositivi di proprietà personale non sono autorizzati ad accedere a tutti i servizi di rete autenticati di GFT, alla connessione a reti GFT interne o reti wireless interne, o alla memorizzazione ed elaborazione in qualsiasi forma di dati non pubblici di GFT a meno che le informazioni GFT possano essere adeguatamente protette.

I dispositivi mobili non in esecuzione sulla piattaforma GFT MDM, inclusi i dispositivi che non supportano tale soluzione, quelli su cui i proprietari si rifiutano di installarlo o quelli su cui la MDM è disattivata o rimossa dopo l'installazione, non devono essere utilizzati per creare, modificare, archiviare o comunicare tutti i dati non pubblici di GFT.

La Società provvede a mantenere aggiornata la mappatura dei dispositivi mobili assegnati ad ogni risorsa tramite utilizzo di un software che gestisce inventari e assegnazioni (CMDV).

In caso di furti o di smarrimenti dello strumento, l'assegnatario deve attenersi alla seguente procedura:

Comunicare immediatamente l'incidente all'IT locale e del Gruppo;

Comunicare l'incidente a databreach@gft.com

Effettuare presentazione della denuncia alle autorità competenti,

Provvedere a far pervenire copia della medesima all' IT e all'ufficio del personale entro il primo giorno lavorativo successivo alla suddetta denuncia.

In qualsiasi momento GFT ha diritto di cancellare remotamente un dispositivo, ad esempio in caso di un incidente di sicurezza.

I dettagli dei controlli relativi al processo sono contenuti nella Mobile Policy.

h) Rapporti con fornitori esterni

Nel caso di comunicazione ai fornitori o altri soggetti terzi di profili di autorizzazione ai fini di consentire interventi immediati o diretti sul sistema, si rende necessario presenziare all'intervento provvedendo comunque al termine, alla modifica immediata delle credenziali di autorizzazione se immesse o conosciute dall'operatore terzo.

Tutti i fornitori esterni, tramite la sottoscrizione di apposite clausole contrattuali o di dichiarazioni pattizie ad hoc, sono comunque vincolati al rispetto delle policy aziendali in materia di privacy, 231 e sicurezza informatica (Third Parties Information Security Policy).

i) Sicurezza e manutenzione dei sistemi

Sicurezza perimetrale e fisica dei server

L'IT provvede a controllare in modo continuativo, la sicurezza perimetrale e fisica dei server.

Tale obiettivo è perseguito mediante l'allocazione dei server in apposito spazio protetto mediante accesso effettuato solo dai possessori degli appositi dispositivi di accesso.

Ogni visitatore che entri in un'area protetta deve essere accompagnato da un dipendente. Se un fornitore/persona esterna alla Società sta lavorando su apparecchiature, partecipando a riunioni o accedendo ad aree riservate, non deve essere lasciato senza supervisione.

Tutti i programmi che possono costituire oggetto di attacco dagli hacker per penetrazioni sono costantemente aggiornati.

Devono essere mantenuti aggiornati tutti i computer fissi e portatili e comunque tutti i sistemi tecnologicamente idonei ad eccedere alla rete, al fine di prevenire qualsiasi possibile tentativo di attacco.

L'IT imposta le modalità di aggiornamento automatico su tutti i sistemi client.

Deve essere costantemente monitorato il sistema per limitare ogni vulnerabilità da attacchi eventualmente con adozione di "Tecniche di Hardening"

I server interni di sviluppo sono resi accessibili solo tramite connessione interna alla rete o accesso VPN con preventiva autorizzazione del profilo dell'utente informatico assegnatario.

I dettagli dei controlli relativi al processo sono contenuti nella *Physical Security Policy*.

Sicurezza del sistema in locale – antivirus

Ogni computer è dotato di un proprio antivirus che si aggiorna automaticamente via internet.

Il server di posta aziendale è provvisto di un antivirus che analizza le e-mail in ingresso e cancella quelle infette e di un antispam che elimina le e-mail che non provengono da un server di posta canonico (grey list).

Qualora l'utente informatico rilevi anomalie nel funzionamento dell'antivirus, provvede a darne immediata comunicazione all' IT previo salvataggio delle sessioni attive.

L'IT interviene prontamente, anche da remoto, al fine di verificare ipotesi di mancato aggiornamento o contrazione di virus, procedendo nei termini congrui rispetto alla problematica rilevata, all'aggiornamento dell'antivirus o alla rimozione del virus rilevato.

I dettagli dei controlli relativi al processo sono contenuti nella Malware Protection Policy.

j) Collegamento dalla rete GFT alla rete del cliente

I dipendenti GFT che si connettono remotamente alla rete del cliente devono seguire le Policy e gli standard di sicurezza GFT e le Policy e gli standard del cliente. I dipendenti GFT devono segnalare qualsiasi evento o incidente legato alla sicurezza.

Il trasferimento di informazioni del cliente su connessioni VPN locali GFT devono essere approvate prima di essere eseguite. È consentito utilizzare solo tipologie di connessioni cliente approvate per accedere ai sistemi e servizi degli stessi.

La connessione VPN del cliente deve essere utilizzata solo per accedere a servizi o sistemi approvati necessari per soddisfare le necessità dei business.

k) Sviluppo sicuro di Software

I team di sviluppo devono utilizzare le migliori tecniche di sicurezza e norme riconosciute nello sviluppare dei software, tra cui standard di codifica sicuri per ogni linguaggio di programmazione utilizzato e configurazione sicura dei sistemi operativi.

Ambienti di sviluppo, integrazione e produzione dovrebbero essere separati e le esigenze di accesso ai dati ed il principio del minimo privilegio eseguiti.

I team di sviluppo devono selezionare i dati relativi ai test evitando accuratamente quei dati che contengono informazioni personali identificabili o altre informazioni sensibili. A tal fine, per nascondere o rimuovere dati sensibili deve essere utilizzato un processo di mascheratura dei dati.

Se a causa di problemi operativi devono essere utilizzati dei dati personali, devono essere osservate le seguenti linee guida:

- L'uso di informazioni personali o sensibili deve essere registrato per fornire possibilità di controllo, compreso il personale specifico che ha accesso a queste informazioni;
- I dati devono essere rimossi immediatamente dopo aver completato il test;
- L'uso di PII (informazioni di identificazione personale) deve essere comunicato e approvato dai Responsabili della Protezione Dati e dai Responsabili della Sicurezza dell'Informazione.

Nel caso in cui qualsiasi cliente adotti Policy, norme e/o requisiti di sicurezza per lo sviluppo del software, la Policy GFT è complementare e non dovrebbe essere esclusa.

I dettagli dei controlli relativi al processo sono contenuti nella Secure Development Policy.

l) Gestione degli incidenti di sicurezza informatica

L'“incidente di sicurezza nella gestione delle informazioni” è un evento avverso o una vulnerabilità che ha causato o ha il potenziale di causare danni ai beni di un'organizzazione, reputazione e/o al personale. La gestione degli incidenti prevede l'intrusione, compromissione e l'uso improprio di informazioni e risorse di informazioni e la continuità dei sistemi e processi di informazione critica.

Un incidente di sicurezza informatica include ma non è limitato ai seguenti: la perdita o il furto di dati e di informazioni, il trasferimento di dati o informazioni a coloro che non hanno diritto di ricevere tali informazioni, tentativi (falliti e/o riusciti) volti ad ottenere l'accesso non autorizzato ai dati o alle informazioni, mancato rispetto delle norme etc.

Tutti gli individui devono riferire immediatamente qualsiasi evento o vulnerabilità di sicurezza osservato o sospetto all'indirizzo databreach@gft.com

Il personale GFT deve limitarsi a riferire e non tentare di testare una vulnerabilità di sicurezza, poiché tale azione può essere considerata una violazione della Policy di sicurezza dell'informazione.

I dettagli dei controlli relativi al processo sono contenuti nella *Information Security Incident Management Policy*.

Le Policy e le Procedure degli incidenti del Cliente devono essere comunque seguite.

m) Gestione delle licenze software

L'acquisto e l'installazione di software con licenza segue un processo operativo ed un flusso di approvazione strutturato che parte dall'apertura di un ticket di richiesta ed arriva, previa verifica tecnica da parte del Chief Technology Officer (CTO), fino all'approvazione da parte del COO.

In particolare, per quanto riguarda il **processo operativo**:

- gli utenti presentano richiesta tramite apertura di ticket a sistema– indicando una categoria specifica – che viene assegnata al team "Admin" dell'IT;

- il team valuta la richiesta in base alla necessità e verifica, mediante accertamento del copyright sulla licenza, se il software è “free use” o “commercial use”;
- se il software è “free use”, la richiesta viene trasferita al team IT per il supporto nell'installazione;
- se, invece, è “commercial use”, viene attivato l'iter approvativo: inizia una procedura formale – richiesta, valutazione, autorizzazione – che coinvolge i responsabili competenti per autorizzare l'acquisto/installazione.

La responsabilità dell'approvazione/installazione dei software con licenza è in capo al CTO, mentre il Responsabile IT, viene inserito nella chain di comunicazioni relative alle aperture dei ticket per conoscenza, in quanto responsabile del centro di costo.

A questo punto, l'applicazione/software è scaricabile dal Company Portal direttamente dall'utente che ha ricevuto l'autorizzazione ovvero dai componenti del team IT con privilegi amministrativi nel caso servisse supporto all'utente.

In tema di vigilanza, GFT utilizza strumenti messi a disposizione dal Gruppo per monitorare quotidianamente i software installati sui dispositivi, con particolare attenzione agli utenti dotati di diritti amministrativi.

n) Utilizzo dell'intelligenza artificiale

Con riferimento all'utilizzo dell'intelligenza artificiale, GFT può rivestire sia il ruolo di fornitore, sviluppando applicazioni mediante l'utilizzo di modelli di intelligenza artificiale di terze parti, sia di deployer avendo integrato nella propria infrastruttura sistemi di intelligenza artificiale.

La ownership tecnica per la diffusione dell'IA all'interno della Società – nonché nell'ambito dello sviluppo di un progetto per un cliente – è affidata all’*“AI Adoption Team”* guidato dal CTO.

Sono stati nominati degli *AI Ambassador* come facilitatori e promotori per l'adozione dell'IA all'interno dei team e dei progetti di delivery nonché viene svolta attività di formazione e sensibilizzazione.

La Società ha implementato una sezione specifica della intranet aziendale dedicata all'AI all'interno della quale è presente, tra l'altro, l'elenco degli strumenti di IA approvati/tollerati/non raccomandati/proibiti, con indicazione specifiche sui costi, use case, caratteristiche principali, stato dell'utilizzo ed indicazione sulle pratiche vietate.

A livello di Gruppo, GFT ha inoltre definito un processo di approvazione di nuovi use cases che prevede una fase di identificazione da parte di una qualsiasi risorsa interna, la condivisione con l'*AI Ambassador* di riferimento, la validazione degli stessi – in caso siano ritenuti di rilevanza aziendale – da parte del CMC (*Change Management Committee*) o del COO/CTO, la standardizzazione degli use cases e la successiva pubblicazione nell'AI Toolbox rendendoli disponibili a tutte le risorse aziendali.

In tema di linee guida/procedure, GFT ha caricato nel proprio SharePoint le *“AI. Centric Guidelines”* che includono indicazioni tecniche, normative ed etiche in merito all'utilizzo dell'intelligenza artificiale.