

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

# Procedura Operativa

## UTILIZZO DEGLI STRUMENTI INFORMATICI

	<b>Funzione</b>	<b>Nominativo</b>
Elaborato	ICT Security	Mario Mangano
Validato	Organization & labour cost	Andrea Sansoni
Verificato	Legal & Corporate Affairs	Primiano De Maria
Verificato	Human Capital & Organization, Health & safety	Alberto Valenza
Verificato	Datore di Lavoro	Marco Troncone
Autorizzato	Information & Communications Technology	Emiliano Sorrenti

Per recepimento delle Società Controllate

	<b>Società</b>	<b>Nominativo</b>
Validato	Datore di Lavoro Airport Cleaning	Raimondo Antonelli
Autorizzato	Consigliere Delegato di Airport Cleaning	Marco Sbrenni
Validato e Autorizzato	Consigliere Delegato e Datore di Lavoro di ADR Mobility	Antonio Fraccari
Validato e Autorizzato	Consigliere Delegato e Datore di Lavoro di ADR Security	Stephane Rabuffi
Validato ed Autorizzato	Consigliere Delegato e Datore di Lavoro di ADR Ingegneria	Maurizio Martignago

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

<b>FLUSSO APPROVATIVO ALLEGATI</b>					
<b>N°</b>		<b>Funzione</b>	<b>Nominativo</b>	<b>Data</b>	<b>Firma</b>
1-2	Autorizzato	ICT Security	Mario Mangano		

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

## Cronologia delle revisioni

N° versione	Data approvazione	Motivo della revisione	Paragrafi modificati
1.0		Annullamento e sostituzione delle seguenti procedure: 1) Gestione delle stazioni di lavoro (P.OPE-ADR/AIT-001), 2) Abilitazione alle reti intranet- internet (P.OPE - ADR/AIT - 002); recepimento azioni di mitigazione della gap analysis Privacy	
1.1		Revisione parziale del processo relativo all'utilizzo degli strumenti informatici; integrazioni in materia di privacy	Tutti
1.2		Aggiornamento per assegnazione posta elettronica a tutti i dipendenti (anche operativi) e utilizzo di delle piattaforme informatiche di collaborazione, integrazioni privacy	Tutti

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

## Indice

1. SCOPO E CAMPO DI APPLICAZIONE .....	5
2. ABBREVIAZIONI .....	5
3. PRINCIPI GENERALI E REGOLE DI FUNZIONAMENTO .....	5
4. RESPONSABILITÀ E COMPETENZE .....	7
5. DESCRIZIONI ITER PROCEDURALE.....	8
5.1 Assegnazione degli Strumenti Informatici .....	8
5.2 Richiesta dei servizi di rete .....	8
5.3 Comportamento in presenza di anomalie e malfunzionamenti .....	9
5.4 Cessazione Del Rapporto Di Lavoro .....	10
6. USO DEGLI STRUMENTI INFORMATICI .....	10
6.1 Personal computer .....	10
6.2 Dispositivi di memorizzazione rimovibili .....	11
6.3 Posta elettronica / e-mail .....	11
6.4 Internet - intranet .....	12
6.5 Utilizzo di social network.....	13
6.6 Utilizzo di piattaforme informatiche di collaborazione (ad es. riunioni online, videoconferenze, messaggistica) .....	14
6.7 Nas – file sharing.....	15
6.8 Produzione di stampe .....	16
6.9 Telefono fisso.....	16
6.10 Comunicazioni via fax .....	16
6.11 Utilizzo di videocamere, macchine fotografiche, registratori di suoni .....	16
7. Informativa per il lavoratore .....	17
8. DEFINIZIONI.....	18
9. RIFERIMENTI NORMATIVI.....	21
10. ALLEGATI.....	22

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

## 1. SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è definire i principi, le responsabilità e le modalità operative relative all'utilizzo degli Strumenti Informatici tangibili (e.g. Personal computer, tablet, palmari, etc.) e intangibili (e.g. internet, mail, cartelle di rete condivise, applicativi) messi a disposizione degli utenti.

La procedura si applica ad ADR e a tutte le Società del Gruppo ADR/Atlantia che hanno attivo un contratto di service con ADR, nello specifico alla data di emissione della presente procedura sono:

- ADR Assistance
- ADR Ingegneria
- ADR Mobility
- ADR Security
- ADR Tel
- Airport Cleaning
- Fiumicino Energia (in virtù del contratto di service).

Non rientrano nel campo di applicazione i telefoni mobili aziendali, regolati da apposita policy. Tuttavia, se non in contrasto con la policy dedicata, l'utilizzo degli strumenti informatici intangibili si applica anche nell'uso dei telefoni mobili aziendali.

## 2. ABBREVIAZIONI

Ai fini della presente procedura valgono le seguenti abbreviazioni:

HRO	Human Capital & Organization, Health & safety
ICO	Information & Communications Technology
TEI	Network & Infrastructures (all'interno di ADR Tel)
RLE	External relations & Sustainability

## 3. PRINCIPI GENERALI E REGOLE DI FUNZIONAMENTO

Il personale della Società è tenuto ad osservare le modalità e i principi esposti nella presente procedura, le pertinenti norme di legge e regolamentari vigenti e applicabili e la pertinente documentazione organizzativa e normativa vigente e applicabile al Gruppo ADR.

Il mancato rispetto di quanto sopra ha rilevanza disciplinare e, pertanto, potrà dar luogo all'irrogazione delle sanzioni previste dalla legge e dal vigente CCNL.

Nello svolgimento delle attività relative al processo descritto devono essere osservati i seguenti principi generali:

<i>Procedura Operativa</i>	<i>Versione</i>	<i>Data</i>
UTILIZZO DEGLI STRUMENTI INFORMATICI	1.2	18.06.2021

- le responsabilità e le attività attribuite alle varie unità della Capogruppo possono essere dalle stesse esercitate e svolte, in virtù di contratti di service, anche per le altre Società del Gruppo ADR;
- l'utilizzo degli Strumenti Informatici messi a disposizione degli utenti della Società deve sempre ispirarsi ai principi di diligenza e correttezza. Le suddette risorse oltre a rappresentare un bene aziendale sono anche lo strumento utilizzato per il trattamento di dati di interesse aziendale. Pertanto, tutti gli Strumenti Informatici si considerano strumenti di lavoro e devono essere utilizzati per le sole ed esclusive finalità connesse all'adempimento delle mansioni lavorative affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Infatti, se utilizzati in modo non appropriato, gli Strumenti Informatici possono non solo compromettere la riservatezza, integrità e disponibilità delle informazioni memorizzate, ma anche impedire l'operatività e compromettere la rete aziendale cui sono eventualmente collegate;
- l'utilizzo di software non licenziato è proibito;
- tutto il software presente sugli Strumenti Informatici deve essere preventivamente autorizzato da ICT e installato da quest'ultimo. Eventuali eccezioni devono essere preventivamente autorizzate da ICT;
- dati di interesse aziendale devono essere memorizzati sui sistemi centralizzati (es. NAS, Sharepoint, documentali aziendali, etc...)
- gli strumenti informatici portatili devono essere opportunamente protetti e gestiti in quanto sono esposte al rischio di furti che comportano un danno non limitato al semplice valore intrinseco del bene, ma comprendente anche la violazione delle informazioni aziendali in esse contenute.

Con riferimento alla violazione della normativa in materia di responsabilità delle persone giuridiche è fatto divieto di:

- porre in essere comportamenti che possano rientrare nelle fattispecie di reato di cui all'art. 24-bis del D.lgs. 231/2001 quali, a titolo meramente esemplificativo e non esaustivo:
  - introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso
  - detenere e diffondere abusivamente codici di accesso a sistemi informatici;
  - accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
  - diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
  - intercettare, impedire o interrompere illecitamente le comunicazioni informatiche o telematiche;
  - installare apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
  - distruggere, deteriorare, cancellare, alterare informazioni, dati e programmi informatici, anche di pubblica utilità.

<i>Procedura Operativa</i> UTILIZZO DEGLI STRUMENTI INFORMATICI	<i>Versione</i> 1.2	<i>Data</i> 18.06.2021
--	------------------------	---------------------------

- porre in essere comportamenti in violazione della normativa relativa al diritto d'autore.

Relativamente alla gestione dei dati personali trattati con Sistemi Informatici è fatto obbligo al personale del Gruppo ADR di:

- trattare i dati personali ed informazioni aziendali in modo lecito, corretto e trasparente, in accordo a quanto prescritto nelle procedure e nelle comunicazioni aziendali e nei limiti delle funzioni lavorative di relativa competenza;
- effettuare l'accesso ai dati personali solo se autorizzati, per finalità strettamente necessarie, pertinenti e non eccedenti lo svolgimento della propria mansione;
- segnalare senza ritardo al Referente Privacy Interno l'esistenza di un trattamento di dati personali per finalità o modalità diverse da quelle autorizzate e comunicare immediatamente per iscritto al Referente Privacy Interno qualsiasi atto, omissione o circostanza, evento, da chiunque commesso, che possa costituire una violazione dell'integrità, confidenzialità e disponibilità dei dati personali;
- realizzare quant'altro sia utile e/o necessario al fine di garantire l'adempimento di tutti gli obblighi previsti dalla normativa, nei limiti delle mansioni lavorative svolte.

Salva specifica autorizzazione scritta proveniente dal Referente Privacy Interno al personale del Gruppo ADR non è consentito:

- effettuare, estrazioni o copie di dati personali non coerenti con le finalità del trattamento;
- permettere, per alcuna finalità, l'accesso ai dati sui sistemi informatici da parte di soggetti terzi, anche colleghi, non espressamente autorizzati;
- cedere a terzi i dati presenti nelle banche dati o copia, totale o parziale, degli stessi, fatta eccezione per eventuali necessità derivanti da operazioni disciplinate da opportune procedure aziendali;
- creare nuove e/o autonome banche dati, se non espressamente autorizzate.

Qualora le attività aziendali, o parti di esse, del processo in oggetto fossero affidate a società terze, è responsabilità del Responsabile della Gestione del Contratto operare un adeguato governo delle terze parti in modo da garantire la piena rispondenza ai requisiti definiti nella presente procedura.

Inoltre, la Società richiede la massima riservatezza delle notizie, dati e informazioni che costituiscono il patrimonio aziendale o che riguardano il business.

## 4. RESPONSABILITÀ E COMPETENZE

In aggiunta alle responsabilità riportate nella descrizione dell'iter procedurale:

**ICO** è responsabile di garantire l'adozione delle misure di sicurezza informatiche adeguate sensibilizzando i soggetti interessati/utenti utilizzatori al rispetto delle regole relative al corretto utilizzo degli Strumenti Informatici. L'obiettivo delle suddette regole è quello di evitare condotte

<i>Procedura Operativa</i> UTILIZZO DEGLI STRUMENTI INFORMATICI	<i>Versione</i> 1.2	<i>Data</i> 18.06.2021
--	------------------------	---------------------------

che, anche solo per negligenza o imprudenza, possano determinare un danno effettivo o potenziale sia allo strumento utilizzato sia ai dati e/o servizi dallo stesso forniti.

**ADR TEL** è responsabile di assegnare i profili di utilizzo Internet/Intranet.

Le unità coinvolte nel processo descritto nella presente procedura sono responsabili di assicurare la tracciabilità e archiviare la documentazione di competenza.

## 5. DESCRIZIONI ITER PROCEDURALE

### 5.1 Assegnazione degli Strumenti Informatici

La richiesta di assegnazione degli Strumenti Informatici deve essere inoltrata a ICT tramite Sistema di IT Provisioning o, qualora non disponibile, l'apposito modulo disponibile sulla intranet aziendale.

In considerazione dei tempi tecnici necessari per l'allestimento e configurazione di quanto necessario per il funzionamento degli Strumenti Informatici, le richieste devono pervenire con almeno sette giorni lavorativi di anticipo rispetto alla data della prevista operatività.

Alla consegna dello Strumento Informatico ICT rilascia il report di installazione che attesta la consegna e il corretto funzionamento degli Strumenti Informatici consegnati. Il suddetto report riporta in sintesi tutte le informazioni inerenti alla fornitura ivi compresi i dati dell'utente utilizzatore (Cognome, Nome, Ente di appartenenza etc.). Il modulo di cui sopra a firma dell'utente / ICT viene rilasciato in copia all'utente.

A fronte della suddetta fase, ADR Tel registra sul sistema di Trouble Ticketing BMC le informazioni relative al nome dell'assegnatario, della postazione di lavoro o del telefono aziendale.

L'iter sopra riportato è da considerarsi valido anche per le modifiche a Strumenti Informatici esistenti, ove per necessità legate alle singole attività se ne dovesse richiedere la variazione.

Relativamente alla richiesta di assegnazione del profilo di un'utenza, si rinvia alla procedura *Gestione degli accessi logici ai sistemi informatici*.

### 5.2 Richiesta dei servizi di rete

L'utente, attraverso il Sistema di IT Provisioning o tramite apposito modulo disponibile sulla intranet aziendale, può richiedere alcuni servizi aggiuntivi. I servizi aggiuntivi che possono essere richiesti sono:

- account di dominio (per l'autenticazione di rete);
- casella di posta aggiuntiva;
- modifica abilitazioni per:
  - accesso ad internet;
  - autorizzazioni cartelle condivise – NAS e relativi diritti.
- installazione SW in base alle attività assegnate.

La richiesta è sottoposta a verifica da parte del Responsabile dell'unità ed eventualmente a successiva validazione dell'Application Owner (qualora si faccia riferimento a software o moduli di essi).

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

Sarà compito di ICT/ADR TEL, mediante specifica attività di monitoraggio periodico, verificare la corrispondenza tra le licenze software acquistate e le licenze software installate sulle postazioni di lavoro. Tale attività verrà effettuata tramite strumento automatico di asset management.

Nello specifico si evidenzia che l'accesso ad intranet/internet attraverso un terminale aziendale è consentito in accordo ai seguenti profili di abilitazione:

- Open: accesso libero a intranet/internet, con limitazione per alcune categorie di siti/file (indicate nell'Allegato1);
- Restricted: accesso limitato all'intranet aziendale e ai siti delle Società del Gruppo ADR.

L'assegnazione dei suddetti profili di abilitazione avverrà secondo i seguenti criteri:

- Open, assegnato per default a tutti gli utenti in possesso di un account di accesso assegnato individualmente e nominativo
- Restricted, assegnato per default alle utenze di presidio generiche.

HRO, su proposta della unità/Società coinvolta, valuta eventuali richieste in deroga alle configurazioni di default (richiesta di estensione a siti/contenuti o file non previsti nel profilo open) che potranno essere gestite attraverso il Sistema di IT Provisioning o tramite apposito modulo Richiesta nuove configurazioni (Allegato 2), da inviare all'unità tecnica Servizi IT.

Il processo di assegnazione del profilo di utilizzo intranet/internet è assicurato operativamente da ICT, sulla base della tipologia di postazione interessata dalla richiesta e dei criteri sopra descritti.

### 5.3 Comportamento in presenza di anomalie e malfunzionamenti

L'assegnatario degli Strumenti Informatici deve comunicare qualunque tipo di anomalia o malfunzionamento mediante lo strumento di IT Provisioning, qualora disponibile, o chiamando il centralino USER SUPPORT (Tel. 5151) o inserendo la segnalazione tramite portale MyIT.

Al fine di permettere una più precisa individuazione del malfunzionamento o dell'anomalia e una maggiore rapidità ed efficienza per l'immediata valutazione, l'assegnatario fornisce una descrizione del malfunzionamento o dell'anomalia. Di seguito alcuni esempi di malfunzionamenti:

- lo Strumento Informatico non si accende;
- Problematiche di accesso – Utente e Password;
- Un software del pacchetto Office non funziona correttamente;
- Outlook non funziona correttamente;
- Il Browser non funziona correttamente
- il PC è guasto o danneggiato
- le informazioni sull'ultimo LOGIN effettuato non corrispondono all'ultima connessione di rete realizzata dall'utente

<i>Procedura Operativa</i> UTILIZZO DEGLI STRUMENTI INFORMATICI	<i>Versione</i> 1.2	<i>Data</i> 18.06.2021
--	------------------------	---------------------------

- l'accesso ai servizi di rete non è disponibile
- la comparsa di messaggi strani sul video imputabili a virus è riconducibile ad un'anomalia.

#### 5.4 Cessazione Del Rapporto Di Lavoro

In caso di cessazione per qualsiasi motivo del rapporto di lavoro, a prescindere da che si tratti di dipendenti o lavoratori ad altro titolo del Gruppo ADR, l'Utente in questione deve restituire qualsiasi risorsa gli fosse stata assegnata, sia con riferimento agli Strumenti Informatici sia, più in generale, al patrimonio informativo a lui fornito.

A seguito della cessazione del rapporto di lavoro verranno seguite le modalità descritte nella procedura *Gestione degli accessi logici ai sistemi informatici*.

La restituzione di telefoni mobili aziendali segue quanto indicato nella Policy "utilizzo dei telefoni mobili aziendali".

HRO coordina la restituzione degli strumenti del dipendente uscente e comunica alla società ADR Tel la disabilitazione della casella di posta.

## 6. USO DEGLI STRUMENTI INFORMATICI

### 6.1 Personal computer

L'assegnatario è responsabile di:

- custodire diligentemente sia all'interno che all'esterno delle sedi aziendali il computer portatile (ma anche palmari, e/o tablet) evitando di lasciarlo incustodito (spazi ad accesso pubblico) anche per brevi periodi;
- garantire che lo schermo del desktop/laptop sia bloccato e protetto da password ogni volta che ci si allontana dallo stesso. In ogni caso le misure di sicurezza ICT prevedono l'attivazione automatica dello screen saver dopo alcuni minuti di inattività. Con riferimento a palmari e tablet, prevedere meccanismi di blocco automatico dello schermo con sblocco mediante PIN, password o misura più robusta (es. lettore impronta digitale);
- scegliere, per la creazione di una password, l'unione di due o più parole non correlate ed effettuando la sostituzione di alcune lettere con numeri o simboli (es. Marz0fin3str@) o scegliere le iniziali delle parole di una frase facile da ricordare (es. versi di una poesia, titolo di una canzone, etc.) ed effettuare la sostituzione di alcune lettere con numeri o caratteri speciali;

Inoltre:

- non è consentito l'uso di programmi diversi da quelli ufficialmente installati da ICO né viene consentito, di norma, agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti;
- salvo preventiva espressa autorizzazione di ICO, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione (6.2), comunicazione o altro (come ad esempio masterizzatori, modem,

<i>Procedura Operativa</i> UTILIZZO DEGLI STRUMENTI INFORMATICI	<i>Versione</i> 1.2	<i>Data</i> 18.06.2021
--	------------------------	---------------------------

etc.). La configurazione base di pc e client non può essere alterata se non a fronte di richieste specifiche derivanti da giustificate esigenze operative;

- non è consentita la memorizzazione di file contenenti dati personali all'interno delle cartelle locali dei PC se non strettamente necessario per svolgere la propria attività lavorativa. In ogni caso tale necessità andrà comunicata a ICO che valuterà la soluzione più sicura da adottare.

## 6.2 Dispositivi di memorizzazione rimovibili

Se, per una determinata esigenza lavorativa, in assenza di strumenti alternativi più sicuri (es. mail, sistema di file sharing autorizzato dal responsabile di ICO, etc.), l'utilizzo di tali dispositivi è consentito rispettando le seguenti indicazioni:

- prestare massima attenzione ai file contenuti in chiavette USB. In particolare non utilizzare chiavette USB di provenienza non nota avvertendo immediatamente il personale IT;
- avere cura delle chiavette USB per evitarne lo smarrimento.

## 6.3 Posta elettronica / e-mail

La e-mail è uno strumento di comunicazione a supporto del business aziendale e per il suo utilizzo è necessario, in generale, che l'assegnatario utilizzi la normale diligenza che si applica alle altre attività lavorative.

La email è assegnata a tutti i dipendenti del Gruppo ADR (area staff e operativa) tramite uno specifico account (al quale è assegnata una casella di posta elettronica individuale con specifico format ad es. nome.cognome@dominiosocietario.it o altro format) per inviare e ricevere messaggi, attinenti l'attività lavorativa svolta, sia internamente alla Società che all'esterno (clienti, fornitori, società, PA, etc.). Per i dipendenti delle aree operative, l'accesso alla casella postale avviene tramite il web browser.

Il sistema di posta elettronica è disponibile, per esigenze specifiche, anche per utenti esterni.

L'utilizzo di posta elettronica da parte di dipendenti di società esterne è regolamentato, tra le parti, in sede contrattuale.

L'assegnatario è tenuto a prestare la massima attenzione alle mail ricevute verificando prima di aprirle, l'oggetto, il mittente ed eventuali file allegati.

Al fine di un corretto uso degli Strumenti Informatici, l'assegnatario è invitato a non utilizzare l'e-mail per l'invio di messaggi non strettamente connessi con l'attività lavorativa e la gestione del rapporto di lavoro. In particolare non è consentito all'assegnatario:

- spedire e-mail che possano risultare diffamatorie, oscene e offensive o che possano essere considerate da altri fonte di discriminazione religiosa, razziale, sessuale, politica, sindacale;
- l'invio massivo di comunicazioni che non siano state autorizzate, compresi i messaggi a sfondo sociale/umanitario. Qualora si dovesse presentare la necessità, rivolgersi all'unità preposta alla comunicazione per le iniziative sociali;
- spedire messaggi o documenti che possono recare danno alla Società;

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

- spedire e-mail indesiderate a fini commerciali non attinenti l'attività lavorativa (spamming);
- spedire e-mail che, per forma o contenuto, possano ledere l'immagine della Società o compromettere le relazioni con clienti, fornitori o terzi;
- l'utilizzo della funzione "Rispondi a tutti", se non quando strettamente necessario;
- iscriversi a servizi web (Social, newsletter, etc..), salvo le esclusioni di cui al paragrafo 6.5 della presente procedura;
- partecipare a catene telematiche o di qualunque altro genere;
- memorizzare o inviare materiale che violi il copyright o altre leggi sul diritto d'autore o sulla proprietà industriale;
- l'utilizzo della posta elettronica per comunicazioni interne aventi come scopo la consegna di credenziali di accesso a sistemi, data base o applicazioni di produzione. Fa eccezione l'invio della sola password in seguito ad operazioni di reset che richiedono il cambio al primo accesso.

Inoltre, non è consentito inviare a terzi informazioni riservate, o contenenti dati personali, particolari e/o giudiziari tramite e-mail. Tuttavia, laddove si avesse l'esigenza di inviare messaggi di natura riservata contenente tali tipologie di dati, si raccomanda di garantirne la protezione utilizzando adeguati meccanismi di cifratura o richiedendo il supporto della competente funzione ICT. Un esempio di condivisione sicura è l'invio di file protetti con password da inviare separatamente rispetto alla mail contenente l'allegato (es. con un'ulteriore e-mail o con un SMS). Relativamente alle disposizioni da applicare per la gestione delle informazioni aziendali, si rinvia anche alle Linee Guida Classificazione e gestione delle informazioni aziendali.

In caso di assenze (ad es. per ferie o attività di lavoro fuori sede), per tutelare sia il mittente che il destinatario, è consigliato utilizzare il sistema di risposta automatica, che consente di inviare automaticamente messaggi di risposta contenenti la data del programmato rientro in azienda ed in particolare i riferimenti (elettronici e telefonici) di un altro soggetto o altre utili modalità di contatto della struttura o unità di appartenenza.

È facoltà delle funzioni competenti accedere alla casella di posta elettronica del lavoratore nei casi indicati nell'informativa per il lavoratore, punto 7 del presente documento.

## 6.4 Internet - intranet

Con riferimento alla rete internet, l'assegnatario abilitato alla navigazione in rete è responsabile del corretto utilizzo della connessione e, a partire dal momento di attivazione della stessa, tutti i contenuti internet visitati tramite terminale aziendale, si presumono effettuati dall'assegnatario e con il suo consenso.

Pertanto, l'accesso a Internet deve essere effettuato per scopi attinenti alla propria attività lavorativa.

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

A tal fine il soggetto abilitato dovrà effettuare tutte le operazioni che contribuiscono a limitare e/o evitare disservizi e soprattutto minacce alla sicurezza per la società, in quanto un utilizzo improprio dell'accesso alla rete internet, costituisce una violazione delle norme comportamentali.

L'utilizzo di Internet non è consentito per il download di software o altri contenuti protetti da diritti d'autore non dotati di corretta licenza o i cui costi debbano essere addebitati alla società. In particolare, è in ogni caso vietato all'assegnatario accedere a siti i cui contenuti non siano adeguati alla serietà ed al decoro richiesti nei luoghi di lavoro.

Nei casi di anomalie del sistema o di utilizzi impropri di internet, la società può adottare controlli e misure atte a garantire la funzionalità e la sicurezza del sistema.

Il controllo è effettuato in forma anonima e può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo di internet e con l'invito ad attenersi scrupolosamente alle istruzioni impartite. L'avviso viene circoscritto all'unità o all'area aziendale in cui è stata rilevata l'anomalia.

Qualora l'anomalia sussista e comporti un abuso da parte di qualche utenza, la società potrà effettuare controlli a campione sui singoli dipendenti per individuare l'esatta fonte dell'abuso.

Quest'ultimo controllo potrebbe determinare l'acquisizione di dati personali dell'utente e portare all'irrogazione di provvedimenti disciplinari.

A tal proposito si rende noto dell'esistenza del registro elettronico di funzionamento dell'accesso alla rete internet (log), il cui contenuto avrà carattere di riservatezza assoluta e potrà essere esibito esclusivamente su richiesta dell'Autorità Giudiziaria.

Avuto riguardo alla rete intranet, l'assegnatario utilizza il servizio di navigazione intranet esclusivamente tramite il Proxy (si ricorda che è vietato l'uso di modem personali) che ha la funzione di Content Filtering e permette diversi livelli di navigazione. Il Sistema di Content Filtering verifica se la richiesta non viola le categorie di contenuti elencate nell'Allegato 1.

Pertanto l'accesso a Internet deve essere effettuato, da parte dell'assegnatario, per scopi attinenti alla propria attività lavorativa.

## 6.5 Utilizzo di social network

Durante l'orario di lavoro e tramite Strumenti Informatici aziendali è vietato l'utilizzo dei social network.

Le uniche eccezioni a tale principio sono:

- 1) l'utilizzo di social network da parte dei dipendenti delle sole funzioni aziendali autorizzate in ragione delle responsabilità/attività assegnate a quest'ultime (ad es.: HR, Marketing, Commerciale, ...).

I dipendenti autorizzati devono:

- osservare i principi deontologici e rispettare i confini professionali;
- garantire un approccio ed un comportamento che in ogni momento assicuri educazione, professionalità, discrezione e buon senso;
- in caso di eventuali commenti, post e pubblicazioni, mantenersi nell'ambito della buona educazione, in quanto potrebbero avere ripercussioni negative sulla reputazione propria e del Gruppo ADR;
- impostare correttamente le opzioni dei social media relative alla privacy e mantenere separate le informazioni personali da quelli professionali;

<i>Procedura Operativa</i> UTILIZZO DEGLI STRUMENTI INFORMATICI	<i>Versione</i>	<i>Data</i>
	1.2	18.06.2021

- 2) l'utilizzo di WhatsApp<sup>1</sup>, da scaricare su base volontaria e facoltativa da parte dei dipendenti sul telefono mobile aziendale o personale, tramite il quale sono inviate (da numerazione aziendale), informative relative alle iniziative di comunicazione interna istituzionale e di people care, previa attivazione del canale.

L'utilizzo di questo ulteriore strumento di comunicazione non sostituisce i canali tradizionali messi a disposizione dei dipendenti.

Il dipendente potrà, in qualsiasi momento, disattivare il canale di comunicazione WhatsApp (numerazione aziendale), continuando a beneficiare delle comunicazioni aziendali tramite i consueti strumenti (e-mail, intranet, bacheca). I messaggi WhatsApp da numerazione aziendale sono unidirezionali – non è abilitata alcuna funzionalità che consente di dialogare – ed eventuali esigenze del dipendente di rispondere o comunicare con l'azienda potranno essere assolte inviando una mail all'indirizzo presente nei messaggi stessi. Inoltre, si precisa che non si potrà utilizzare WhatsApp (numerazione aziendale) per scambio di messaggi tra dipendenti e che gli stessi sono indirizzati solamente ai singoli destinatari e non devono essere inoltrati/divulgati ad altri soggetti.

In nessun caso, sarà utilizzato WhatsApp per inviare ai dipendenti comunicazioni di carattere personale.

L'utilizzo da parte dei dipendenti del WhatsApp aziendale non deve interferire con il corretto svolgimento delle attività lavorative assegnate (quindi privilegiando la visualizzazione dei messaggi ricevuti durante le pause previste dal CCNL di riferimento o prima dell'inizio del proprio turno di lavoro o dopo il suo termine, ferma restando la necessità di assicurare il rispetto delle regole previste nello svolgimento della mansione propria di ogni dipendente).

Il trattamento dei dati personali avviene nel rispetto della normativa data protection applicabile e con le logiche descritte all'interno dell'informativa privacy appositamente predisposta e resa ai dipendenti ai sensi dell'articolo 13, GDPR.

L'utilizzo di social network fuori dal contesto lavorativo e a fini personali non deve ledere o danneggiare l'immagine aziendale o quella dei suoi referenti / dipendenti.

### 6.6 Utilizzo di piattaforme informatiche di collaborazione (ad es. riunioni online, videoconferenze, messaggistica)

Le piattaforme di collaborazione, ad es. Cisco WebEx, sono messe a disposizione dei dipendenti del Gruppo ADR e consentono principalmente di:

- effettuare riunioni online e videoconferenze
- gestire la messaggistica istantanea
- gestire le chiamate audio e video
- avere a disposizione la funzionalità di collaborazione e condivisione di file e dati aziendali

---

<sup>1</sup> Applicazione di messaggistica istantanea per dispositivi mobili multipiattaforma che, attraverso la connessione a Internet, consente lo scambio tra uno o più utenti di messaggi di testo e file multimediali

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

- di conoscere la disponibilità del dipendente per le attività di collaborazione (ad es. stato attivo, non disturbare).

Al fine di un corretto utilizzo dalle piattaforme informatiche di collaborazione, il dipendente è invitato a non utilizzarle per l'invio di messaggi non strettamente connessi con l'attività lavorativa e alla gestione del rapporto di lavoro.

In particolare non è consentito al dipendente utilizzare la chat per inviare messaggi:

- che possano risultare diffamatori, osceni e offensivi o che possano essere considerati da altri fonte di discriminazione religiosa, razziale, sessuale, politica, sindacale;
- che possono recare danno alla Società;
- indesiderati a fini commerciali non attinenti l'attività lavorativa (spamming);
- che, per forma o contenuto, possano ledere l'immagine della Società o compromettere le relazioni con clienti, fornitori o terzi;
- che contengano materiale che violi il copyright o altre leggi sul diritto d'autore o sulla proprietà industriale;
- per la consegna di credenziali di accesso a sistemi, data base o applicazioni di produzione.

Inoltre non è consentito inviare a terzi, tramite le piattaforme di collaborazione, informazioni riservate o contenenti dati personali, particolari e/o giudiziari. Relativamente alle disposizioni da applicare per la gestione delle informazioni aziendali, si rinvia anche alle Linee Guida Classificazione e gestione delle informazioni aziendali.

Nell'utilizzo della piattaforma, al fine di ottimizzare la collaborazione tra dipendenti, è:

- richiesto in caso di lavoro in modalità smartworking di tenere attiva la funzionalità relativa allo stato di disponibilità del dipendente durante l'orario di lavoro
- richiesto di utilizzare le immagini di corporate identity ADR con le quali personalizzare lo sfondo (backdrop), disponibili sulla intranet nella sezione Corporate identity
- consigliato in riunione o in videoconferenza, quando intervengono gli altri colleghi, di disattivare l'audio.

## 6.7 Nas – file sharing

La cartella di rete (di seguito NAS) è uno spazio messo a disposizione degli assegnatari per la condivisione di file, previa autorizzazione del proprio Responsabile organizzativo. Le cartelle di rete sono aree destinate alla condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Pertanto, l'assegnatario non deve collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa.

I diritti di accesso alle cartelle di rete devono essere sempre coerenti con l'attività lavorativa svolta dagli assegnatari, pertanto in caso di cambiamenti organizzativi l'utente è responsabile di inserire la richiesta di aggiornamento/disabilitazione dei diritti di accesso nell'apposito sistema.

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

## 6.8 Produzione di stampe

L'utente in caso di produzione di stampe:

- deve recuperale nel più breve tempo possibile, soprattutto se elaborate da stampanti di rete o poste al di fuori della stanza dell'utente;
- in caso di scansione e invio tramite mail assicurarsi che:
  - l'indirizzo mail sia corretto per evitare l'invio ad altri destinatari;
  - il documento scansionato non sia accessibile a personale non autorizzato
- in caso di errore nella stampa distruggere il documento;
- distruggerle quando non più strettamente necessarie per le finalità con cui sono state stampate.

Se le stampe contengono dati personali e riservati, l'utente deve adottare adeguate misure che non permettono l'impropria diffusione a ricezione di tali informazioni.

Relativamente alle disposizioni da applicare per la gestione delle informazioni aziendali, si rinvia anche alle *Linee Guida Classificazione e gestione delle informazioni aziendali*.

## 6.9 Telefono fisso

L'utilizzo del telefono aziendale fisso è consentito per scopi attinenti alla propria attività lavorativa, con la dovuta cura e attenzione. Un uso personale limitato del canale telefonico è consentito se:

- non interferisce con le attività lavorative;
- non è utilizzato per la comunicazione di contenuto contrario a norme di legge, all'ordine pubblico o al buon costume;
- non è utilizzato per messaggi che possano arrecare danno all'immagine della società.

## 6.10 Comunicazioni via fax

Nell'effettuare comunicazioni via fax gli utenti devono:

- prima della trasmissione, verificare il numero del fax per evitare l'invio ad altri destinatari;
- adottare, nel caso di invio tramite fax di informazioni riservate, le seguenti precauzioni:
  - presidiare l'apparecchiatura durante la trasmissione del fax;
  - rimuovere il documento dal fax non appena inviato o ricevuto.
- mantenere copia dei fax spediti e dei rapporti di trasmissione, che potrebbero essere utili in caso di controversia;
- nel caso di informazioni confidenziali, oltre a quanto sopra indicato, avvertire telefonicamente dell'invio, anche al fine di assicurarsi dell'avvenuto ricevimento.

## 6.11 Utilizzo di videocamere, macchine fotografiche, registratori di suoni

Non è possibile da parte del dipendente fotografare e/o registrare oggetti o informazioni, indipendentemente dal carattere sensibile o confidenziale, in mancanza di specifica

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

autorizzazione della Società.

Non è possibile fotografare persone e/o registrare conversazioni o momenti aziendali, se non previo consenso dei soggetti ripresi o registrati, e solo su preventiva autorizzazione/approvazione della Società.

## 7. Informativa per il lavoratore

Con il Decreto legislativo, 14/09/2015 n° 151, G.U. 23/09/2015 sono state introdotte rilevanti novità nella disciplina dei controlli a distanza del lavoratore, con un intervento sull'art. 4 dello Statuto dei lavoratori per adeguare la disciplina all'evoluzione tecnologica, nel rispetto delle disposizioni in materia di privacy.

Garanzie poste in materia di divieto di controlli a distanza si applicano agli impianti audiovisivi che possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

Le garanzie non si applicano agli strumenti di lavoro attraverso i quali il lavoratore rende la prestazione lavorativa (in tale ambito rientrano ad esempio i pc, i tablet e i telefoni cellulari) e agli strumenti per la rilevazione degli accessi e delle presenze.

Ai sensi del comma 3 dell'articolo 4, le informazioni raccolte con i mezzi di controllo sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dalla normativa privacy vigente.

Con tale premessa, la Società ottempera alle indicazioni della citata Legge, in termini di informativa all'utente, fornendo nella presente procedura tutte le informazioni necessarie all'interessato per definire il concetto di strumenti di lavoro, i limiti dell'utilizzo consentito di essi, i controlli effettuati dall'azienda su tali strumenti e tramite tali strumenti. Inoltre, sono fornite tutte le informazioni di cui all'art. 13, GDPR nell'informativa privacy resa in fase di instaurazione del rapporto di lavoro.

A seguito della cessazione del rapporto di lavoro verranno seguite le modalità descritte nella procedura Gestione degli accessi logici ai sistemi informatici.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento /sostituzione/ realizzazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Società, tramite ICO e TEI o addetti alla manutenzione, accedere, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico, come indicato nella Policy "Utilizzo dei telefoni mobili aziendali".

In caso di anomalie, ICO e TEI, effettueranno, avvalendosi di fornitori esterni, controlli anonimi che si concluderanno con un avviso generalizzato da parte della funzione che ha richiesto il controllo diretto ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

Non verranno in alcun caso compiuti controlli prolungati, costanti o indiscriminati.

Il personale incaricato che opera in ICO e TEI, per l'espletamento delle proprie funzioni e per garantire la sicurezza del sistema informatico aziendale, ha la facoltà, in qualunque momento, di accedere, avvalendosi di fornitori esterni, ai log di traffico.

Analoghe verifiche possono essere effettuate sulla cronologia dei siti internet acceduti dagli utenti abilitati alla navigazione esterna a fronte del verificarsi di incidenti informatici e/o eventi sospetti. Resta inteso che l'accesso verrà comunque effettuato con modalità tali da evitare qualsiasi forma di controllo a distanza.

In ogni caso, la Società garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi di computer in uso che non siano nelle modalità regolamentate nel presente documento;
- la visione dei contenuti delle comunicazioni tra utenti
- l'utilizzo del canale WhatsApp per le iniziative di comunicazione interna istituzionale e di people care, in particolare la reportistica sull'utilizzo dello stesso, richiesta da HRO o RLE al fornitore esterno, ha scopi di natura esclusivamente statistica ed è effettuata con dati aggregati; la reportistica è quindi priva di evidenza del nome e cognome del dipendente e degli orari di lettura del messaggio.

## 8. DEFINIZIONI

Ai fini della presente procedura valgono le seguenti definizioni:

### Application Owner

Soggetto individuato dal Responsabile primo riporto AD per ADR, o dal Soggetto Apicale della Società Controllata responsabile delle attività supportate dall'applicativo informatico.

### Dato personale (comune)

Qualsiasi informazione riguardante una persona fisica identificata o identificabile "interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente,

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

#### Categorie particolari di dati personali

Dati personali riguardanti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

#### Dati personali relativi a condanne penali e reati (dati giudiziari)

Dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

#### Hardware

Apparecchiature (Pc, workstation, stampanti, ecc.) per l'elaborazione automatica di dati.

#### Internet

Rete mondiale che consiste in un sistema integrato di interconnessione tra computer e reti locali, che consente la trasmissione di informazioni in tutto il mondo.

#### Intranet

Rete interna aziendale usata per facilitare la comunicazione e l'accesso all'informazione, che può essere ad accesso ristretto. A volte il termine è riferito solo alla rete di servizi più visibile, il sistema di siti che formano uno spazio web interno.

#### LAN

Local Area Network - Reti per la trasmissione dati su brevi distanze e ad alta velocità.

#### Malware

Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno.

#### NAS

La NAS (Network Attached Storage) è un dispositivo collegato ad una rete di computer la cui funzione è quella di condividere tra gli utenti della rete una Area di storage (o disco).

#### Password

Chiave personale per l'autenticazione al sistema.

#### Posta elettronica e-mail

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

La posta elettronica, in inglese E-Mail (abbreviazione di Electronic Mail), è un servizio internet grazie al quale ogni utente può inviare o ricevere dei messaggi.

#### Profilo (di utenza)

Insieme delle caratteristiche di un utente che consentono determinate operazioni come la lettura, la scrittura, la modifica su file e applicazioni.

#### Referente Privacy interno

Responsabili pro-tempore di Funzioni/Unità Organizzative aziendali con maggior impatto sul trattamento dei dati, identificati e nominati dal Titolare del trattamento. Il Referente Privacy Interno risulta "responsabile" del trattamento effettuato nella funzione organizzativa di riferimento, con il compito di vigilare sui trattamenti nel loro specifico ambito di designazione per garantire il rispetto della normativa.

#### Responsabile della Gestione del Contratto

- in Ambito Pubblicistico: il Responsabile del Procedimento per la fase di progettazione ed esecuzione;
- in Ambito Privatistico: l'Approvatore della RdA, ovvero il soggetto formalmente identificato nell'ambito del contratto da parte dell'Approvatore.

#### Rete

Una rete (in inglese network) è un insieme di sistemi per l'elaborazione delle informazioni messi in comunicazione fra loro (vedi LAN – Intranet – Internet).

#### Screen Saver

Programma fornito con il sistema Windows che nasconde il contenuto dello schermo e inibisce l'accesso al Pc dopo un certo periodo di inattività stabilito dall'utente.

#### Software

Tutto ciò che può essere eseguito su un Pc. Sistema operativo, programmi, ecc.

#### Strumenti Informatici

Si intendono gli strumenti informatici tangibili (e.g. Personal computer, tablet, palmari, etc) e intangibili (e.g. internet mail, cartelle di rete condivise, applicativi) messi a disposizione degli utenti

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

#### Utente

Dipendente che per lo svolgimento del proprio lavoro utilizza le risorse messe a disposizione dell'azienda ed in particolare dalla rete aziendale.

#### Virus

<b>Procedura Operativa</b> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

Programma, generalmente dannoso, autoreplicante che si attacca ad altri programmi o a parti eseguibili di sistema e utilizzandoli come vettori per infettare altri PC. Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di malware, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan.

## 9. RIFERIMENTI NORMATIVI

### Riferimenti Esterni

Tutte le pertinenti norme di legge e regolamentari vigenti e applicabili, con particolare riferimento a:

- Decreto Legislativo n°196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali e successive integrazioni e modifiche;
- Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
- Decreto Legislativo 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"
- Statuto dei lavoratori: L. 300/1970
- Videosorveglianza - Provvedimento generale - 08 aprile 2010
- Linee Guida del Garante Privacy per posta elettronica e internet del 1° marzo 2007;
- L. 633/1941 (Diritto d'autore).

### Riferimenti Interni

Tutta la pertinente documentazione organizzativa e normativa vigente e applicabile al Gruppo ADR (modelli, regolamenti, procedure, comunicazioni, etc.), con particolare riferimento a:

- Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001
- Codice Etico del Gruppo Atlantia
- Policy Anticorruzione Atlantia
- Procedura organizzativa - Gestione degli accessi logici ai sistemi informatici
- Policy "Utilizzo dei telefoni mobili aziendali"
- Manuale Regolamentare Privacy

<i>Procedura Operativa</i> UTILIZZO DEGLI STRUMENTI INFORMATICI	<b>Versione</b> 1.2	<b>Data</b> 18.06.2021
--	------------------------	---------------------------

## 10. ALLEGATI

### Allegato 1: Tabella di sintesi in caso di utilizzo di internet

Di seguito viene riportata la tabella sinottica, distribuita per profilo di utilizzo internet, soggetti interessati, tipo di abilitazioni e limitazioni:

profilo di utilizzo	soggetti interessati	abilitazioni
<b>open</b>	Tutti i terminali delle postazioni di lavoro con accesso ad internet	<p>Tutto il world wide web ad eccezione delle seguenti tipologie di contenuti: + intranet azienda e società del gruppo</p> <p>Limitazioni internet:</p> <p><b>Categorie vietate</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Adult Sexuality</li> <li><input type="checkbox"/> Advertisements &amp; Pop-Ups</li> <li><input type="checkbox"/> Criminal Activity</li> <li><input type="checkbox"/> Gambling</li> <li><input type="checkbox"/> Games</li> <li><input type="checkbox"/> Illegal Drugs</li> <li><input type="checkbox"/> Intolerance &amp; Hate</li> <li><input type="checkbox"/> Phishing &amp; Fraud</li> <li><input type="checkbox"/> Spam URLs</li> <li><input type="checkbox"/> Spyware</li> <li><input type="checkbox"/> Tasteless &amp; Offensive</li> <li><input type="checkbox"/> Violence</li> <li><input type="checkbox"/> Weapons</li> <li><input type="checkbox"/> Peer-to-Peer</li> <li><input type="checkbox"/> Ringtones/Mobile Phone Downloads</li> </ul> <p><b>Download vietati</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Audio Video Interleave (avi)</li> <li><input type="checkbox"/> MPEG Audio (mp3)</li> <li><input type="checkbox"/> MPEG Video (mpg, mpeg)</li> <li><input type="checkbox"/> Midi (midi)</li> <li><input type="checkbox"/> QuickTime Video (mov)</li> <li><input type="checkbox"/> RealMedia (rm)</li> <li><input type="checkbox"/> Wave (wav)</li> <li><input type="checkbox"/> Windows Media Audio (wma)</li> <li><input type="checkbox"/> Windows Media Video (wmv)</li> </ul>
<b>restricted</b>	UtENZE non nominative di presidio	Intranet aziendale e siti del Gruppo ADR

