REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA

Il presente Regolamento aziendale entra in vigore il 31/05/2021 e riguarda tutto il personale dipendente della A.R.AL. S.p.A.

1. FINALITÀ

A.R.AL. S.p.A. mette a disposizione del proprio personale e di eventuali collaboratori esterni, i seguenti strumenti di lavoro, in funzione del loro ruolo e delle esigenze lavorative:

- strumenti di informatica individuale, quali personal computer e relativi accessori, ecc;
- apparati e servizi condivisi, quali ad esempio, posta elettronica, internet, stampanti e multifunzioni di rete, file server, ecc;
- programmi e procedure gestionali.

Tali risorse costituiscono strumenti di lavoro e devono essere utilizzate per il perseguimento di fini strettamente connessi all'attività lavorativa secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.

Il documento illustra le norme generali di utilizzo di tali risorse che il personale e i collaboratori devono rispettare al fine di mitigare i rischi che un uso improprio degli stessi può determinare alla sicurezza del patrimonio informativo e all'immagine dell'a Società, nonché l'ambito di eventuali verifiche effettuate dal personale addetto riguardo alla funzionalità e sicurezza dei propri sistemi informativi.

In particolare si evidenzia come l'utilizzo delle risorse informatiche per scopi non inerenti all'attività lavorativa possa contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle infrastrutture della Società.

Nella definizione delle norme comportamentali da osservare si è tenuto conto di quanto previsto dalla normativa vigente in materia e, in particolare:

- Regolamento UE 2016/679 e successiva regolamentazione con D. Lgs. 101/2018,
- provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali, in particolare il Provv. 01 marzo 2017 "Linee guida del Garante per posta elettronica e internet",
- circolari dell'Agenzia per l'Italia Digitale (AGID), in particolare la circ. 18 aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015)".

Le disposizioni contenute nel presente documento si applicano a tutti i dipendenti di A.R.AL.

S.p.A. indipendentemente dal tipo di incarico svolto e dalla sede dell'attività, nonché a tutti i soggetti esterni ai quali verranno espressamente riconosciute applicabili (ad esempio collaboratori esterni, stagisti, borsisti, consulenti, fornitori, tecnici di ditte esterne).

2. UTILIZZO DEL PERSONAL COMPUTER AZIENDALE E PORTATILE: I DIVIETI

In funzione del proprio ruolo e delle esigenze organizzative e lavorative, il personale in servizio presso il A.R.AL. S.p.A. è dotato di personal computer e/o altri dispositivi per lo svolgimento di attività connesse agli incarichi lavorativi, nel rispetto delle regole di seguito descritte.

Ogni utilizzo difforme dall'attività propriamente lavorativa e/o per finalità istituzionali, non consentito, può determinare specifiche responsabilità, oltre ad essere causa di eventuali e conseguenti disservizi, costi di manutenzione e minacce alla sicurezza.

Il personal computer e gli eventuali altri dispositivi sono assegnati nominalmente al dipendente che è pertanto responsabile dell'utilizzo di tali strumenti di lavoro che non devono essere adibiti per uso personale o comunque estraneo all'attività aziendale.

Le postazioni di lavoro sono connesse alla rete lan aziendale allo scopo di usufruire dei servizi dell'Ente, accedere agli applicativi gestionali, condividere informazioni, fruire i contenuti Internet.

Per accedere alla rete lan e agli applicativi gestionali l'utente deve utilizzare le sue credenziali assegnate dal designato IT, per il solo primo accesso, consistenti in un codice per la sua identificazione (Nome Utente) associato ad una parola chiave (password). La gestione delle credenziali dopo il primo accesso sono di pertinenza esclusiva ed autonoma dell'utente.

Considerando la natura dei dati trattati, la funzionalità dell'applicativo, oltre alla strutturazione in turni dell'attività connessa all'utilizzo dell'applicativo medesimo, non si ritiene necessario codificare singolarmente l'accesso dell'applicativo, bensì tracciare con i documenti di presenza l'utilizzo del sistema.

Per una corretta gestione delle postazioni di lavoro è prescritto quanto segue:

- le informazioni archiviate nella postazione devono essere esclusivamente quelle inerenti la propria attività lavorativa;
- il salvataggio (backup) dei dati necessari all'attività lavorativa per le postazioni che non memorizzano i propri dati sul file server centrale è di esclusiva responsabilità dell'utente;
- la modifica dei componenti interni (aggiunta, rimozione, sostituzione) delle attrezzature informatiche messe a disposizione e la modifica delle configurazioni software impostate sulle postazioni di lavoro sono di esclusiva competenza del designato IT;
- non è consentita l'installazione di programmi applicativi diversi da quelli già installati sul p.c. dal designato IT, tra gli altri, browser per la navigazione internet e software di office automation. Le richieste di installazione e aggiornamento di ulteriori applicativi rispetto a quelli autorizzati devono essere preventivamente validate dal designato IT in ordine alle necessarie verifiche tecniche. Qualora venissero riscontrati programmi non autorizzati sulle postazioni di lavoro, anche se legali, questi verranno disinstallati dal designato IT;
- non è consentito utilizzare risorse informatiche private (tablet, smartphone, periferiche etc.), salvo preventiva ed esplicita autorizzazione del designato IT; in caso di autorizzazione, l'utente è tenuto a rispettare le configurazioni di sistema dell'Azienda ed il rispetto delle misure minime di sicurezza descritte nella circolare AGID n. 2/2017;
- Non è autorizzato l'uso di pendrive, hard disk esterni, dvd o analoghi supporti di memorizzazione di incerta provenienza che potrebbero causare danni alla postazione di

lavoro;

- non è consentito duplicare documenti contenenti dati personali o sensibili o aziendalmente rilevanti su supporti removibili o su sistemi di rete non gestiti dal personale aziendale (ad es. su cloud esterno);
- è vietata l'installazione non autorizzata di propri dispositivi di connessione come access point, router, print server, modem, ecc alla rete aziendale;
- in caso di smarrimento o furto di dispositivi informatici, oltre a sporgere regolare occorre informare tempestivamente il designato IT comunicando quali dati erano contenuti all'interno;
- in caso di allontanamento anche temporaneo dalla propria postazione di lavoro è necessario attivare un salvaschermo con password o bloccare il personal computer;
- al termine del lavoro devono essere correttamente chiusi tutti gli applicativi e la sessione di lavoro, e devono essere spenti computer, video ed accessori anche al fine di evitare sprechi energetici ed inutile usura del personal computer;
- costituisce buona prassi effettuare con cadenza periodica (almeno ogni sei mesi) la pulizia degli archivi presenti sulla propria postazione e nelle cartelle di rete di propria competenza, con cancellazione dei file inutili o obsoleti. Si deve porre particolare attenzione ad evitare un'archiviazione ridondante con duplicazione dei dati;
- la tutela della gestione locale dei dati presenti sulle stazioni di lavoro personali (personal computer) è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, salvataggi su supporti di rete;
- nel caso in cui esista la necessità di elaborare banche dati in locale, ad esempio su fogli di calcolo o database personali, è necessario adottare le misure di sicurezza idonee a garantire il rispetto della normativa in materia di tutela dei dati personali.
- L'utente è responsabile delle attrezzature che gli sono affidate in uso e pertanto deve provvedere a mantenerle in completa efficienza segnalando tempestivamente al designato IT ogni eventuale problema tecnico e, in caso di dubbio, sulla sicurezza della postazione di lavoro.
- è consentito ai dipendenti portare con sé il personal computer portatile solo ed esclusivamente in caso di trasferte, o missioni di lavoro, lavoro agile: lo stesso deve essere custodito con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

3. UTILIZZO DEL PERSONAL COMPUTER AZIENDALE E PORTATILE: LE NORME DI BUON FUNZIONAMENTO

Al fine di garantire la perfetta efficienza dei sistemi informatici e di limitare i rischi per la sicurezza degli stessi si invitano tutti i dipendenti a rispettare le seguenti regole di buon funzionamento: il personal computer, anche al fine di evitare l'indebito utilizzo dello stesso da parte di terzi, deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio, fatti salvi i casi di lavoro agile per il quale il personal computer deve rimanere necessariamente acceso. Poiché l'accesso alla rete è protetto da password, la stessa deve essere custodita con la massima diligenza dall'assegnatario, il quale non può divulgarla.

I Designato IT o in sua mancanza, la Direzione Aziendale, hanno la facoltà al solo fine effettuare interventi di manutenzione, di accedere ai dati trattati da ciascuno ed archiviati nel personal computer di lavoro.

I destinatari sono responsabili del corretto utilizzo e dell'adeguata custodia delle smart card,

business key e altri dispositivi per il riconoscimento che contengono certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi della Società, e del relativo PIN e altro materiale a corredo.

4. UTILIZZO DELLA RETE AZIENDALE: I DIVIETI E LE NORME DI BUON FUNZIONAMENTO

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono essere in alcun modo utilizzate per scopi diversi.

Per questo motivo:

- nessun file che non sia collegato all'attività lavorativa, può essere dislocato, nemmeno per brevi periodi, sulle unità di rete. Il designato IT o in sua mancanza, la Direzione Aziendale si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà non essere attinenti l'attività lavorativa ovvero essere pericolosi ovvero acquisiti o installati in violazione del presente regolamento sulle unità di rete;
- al fine di risparmiare spazio sui dischi di rete, si raccomanda di tenere ordinate le varie directory, eliminando files inutili, superati o doppioni. Qualora si rendesse necessario, è possibile, contattando l'Amministratore di Sistema, eseguire copie di back-up di detti files su CD-ROM o altro supporto magnetico.

5. UTILIZZO DELLA CASELLA DI POSTA ELETTRONICA:

- Casella di posta elettronica: spazio di archiviazione che contiene i messaggi di posta elettronica ai quali si accede tramite le proprie credenziali.
- Dominio: nome univoco posto dopo il simbolo @ negli indirizzi email che identifica l'organizzazione che lo gestisce
- Lista di distribuzione: un indirizzo di posta elettronica al quale viene associato un elenco di altri indirizzi.
- Posta Elettronica Certificata (PEC): la Posta Elettronica Certificata (PEC) è un tipo particolare di posta elettronica, disciplinata dalla legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale garantendo così il non ripudio. Inoltre costituisce domicilio digitale.
- Revoca: indica l'azione che rende non più accessibile all'utente la propria casella di posta, ma non comporta un intervento sui dati.
- Sottodominio: dominio che identifica un sottoinsieme dell'organizzazione principale.
- Utente: qualunque soggetto che utilizza la posta elettronica fornita da A.R.AL. S.p.A. e in possesso di specifiche credenziali di autenticazione.

La casella di posta elettronica è uno strumento di lavoro affidato esclusivamente per l'esercizio delle funzioni assegnate e pertanto non deve essere utilizzata per uso personale o comunque estraneo all'attività aziendale.

In considerazione di ciò:

- è fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di catene telematiche e comunque di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa, preventiva ed esplicita autorizzazione della Direzione Aziendale;
- è fatto divieto di utilizzare le caselle di posta elettronica aziendale per pubblicità non istituzionale, manifesta o occulta, per comunicazioni commerciali private, per comunicazioni di propaganda politica esterna all'Ente, per partecipare ad appelli e/o petizioni, a giochi e a qualsivoglia altra attività non riconducibile allo svolgimento dell'attività lavorativa, per l'invio di materiale discriminante o lesivo in relazione a razza, sesso, religione, ... per l'invio di materiale che comporti il trattamento di dati personali in violazione della normativa di riferimento, per l'invio di contenuti o materiali che violino i diritti di proprietà di terzi, diffamatori o palesemente offensivi o, in termini generai, per l'invio di altri contenuti illegali.
- è fatto divieto di fornire a terzi che non siano in rapporto di attività di lavoro, anche per motivi di sicurezza, l'indirizzo e-mail dell'Azienda;
- è fatto divieto di vietato utilizzare sui personal computer caselle di posta elettronica esterne, se non preventivamente autorizzate dalla Direzione Aziendale.

Il designato IT e la Direzione Aziendale hanno la facoltà, al solo fine di effettuare interventi di manutenzione garantire l'operatività e la sicurezza del sistema, nonché il costante e corretto svolgimento dell'attività aziendale, di visionare le e-mail in entrata ed in uscita.

Le prescrizioni di cui ai punti precedenti non costituiscono ipotesi tassative essendo suscettibili di applicazione analogica.

Gli utenti, nella consultazione della posta, devono adottare comportamenti che non pregiudichino la sicurezza informatica della Società. In particolare:

- prestare attenzione a messaggi o allegati che provengono da mittenti sconosciuti o poco attendibili e, in caso non si individui il mittente, non aprirli;
- non aprire allegati di messaggi di posta con estensione eseguibile (ad es. .exe, .bat, .com);
- disattivare l'anteprima automatica dei messaggi;
- disattivare l'anteprima automatica dei contenuti dei file allegati.

La casella di posta elettronica, in quanto strumentale allo svolgimento ordinario dell'attività lavorativa, deve essere consultata regolarmente dall'utente, il quale provvedere a mantenerla in ordine cancellando i messaggi ritenuti inutili e quelli con allegati ingombranti. E' possibile utilizzare, la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, fermo restando che per la comunicazione ufficiale è obbligatorio avvalersi di conferma scritta. Per la trasmissione di file all'interno della stessa sede è preferibile l'utilizzo delle unità di rete piuttosto che allegare il documento ad un messaggio di posta elettronica;

in caso di e-mail, ricevute o da inviare, con contenuto di rilievo per la Società (ad esempio impegni contrattuali o precontrattuali, proposte commerciali, etc.), è necessaria, salvo diverse intese, la preventiva visione e/o autorizzazione da parte della Direzione Aziendale; in ogni caso vanno osservate le procedure in essere presso la Società per la corrispondenza cartacea ordinaria.

Si ricorda inoltra che di tutte le e-mail (in/out) inviate attraverso il server, ne viene mantenuta automaticamente una copia nel server stesso. Si suggerisce in ogni caso di archiviare all'interno delle relative pratiche una copia cartacea delle e-mail rilevanti.

Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati trattati, nel rispetto della normativa vigente, in caso di assenze programmate o prevedibili superiori a 3 giorni lavorativi, l'utente deve predisporre l'invio automatico di un messaggio contenente i recapiti di un altro soggetto o altre utili modalità di contatto della struttura.

In caso di assenze prolungate non programmate e non prevedibili superiori a 3 giorni lavorativi, la Direzione Aziendale, a tutela del buon andamento e dell'efficienza dell'attività istituzionale, che abbia necessità di accedere ai messaggi giacenti nella casella di posta elettronica del dipendente, come previsto dalle "Linee Guida dell'Autorità Garante per posta elettronica e internet" emesse dall'Autorità Garante per la Protezione dei Dati Personali in data 01/03/2007, può chiedere all'utente di:

- provvedere personalmente alla lettura dei messaggi, comunicandone il contenuto rilevante per l'attività lavorativa, e di attivare successivamente la funzionalità di invio automatico di messaggi contenenti i recapiti di un altro soggetto o altre utili modalità di contatto della struttura presso la quale opera il lavoratore assente;
- delegare un altro dipendente (fiduciario) a verificare il contenuto dei messaggi di posta elettronica e a inoltrare alla Direzione Aziendale quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere informato l'utente al suo rientro in servizio.
-

6. UTILIZZO DELLA RETE LOCALE, INTERNET E AREE CONDIVISE

Per l'uso dei servizi connessi ad internet, alla rete locale ed alle risorse di rete condivise, valgono le seguenti norme comportamentali:

- l'accesso a internet è riconosciuto esclusivamente per l'esercizio delle funzioni assegnate e pertanto non deve essere utilizzato per uso personale o comunque estraneo all'attività aziendale;
- non trasferire sulla propria postazione di lavoro, mediante download, file o programmi da siti sconosciuti che potrebbero compromettere il funzionamento del computer o della rete aziendale;
- non scaricare e/o scambiare materiale protetto da diritti di proprietà intellettuale senza averne titolo, e comunque sempre e solo per attività connesse alle esigenze lavorative;
- non è consentito l'uso di programmi peer-to-peer per lo scambio di file in ambito privato;
- non partecipare, a meno di esigenze professionali, a siti di chat, forum e/o social network;
- non pubblicare testi, immagini o video a contenuto blasfemo, osceno o diffamatorio;
- è vietata ogni forma di registrazione, a nome della Società fornendo i dati relativi ad e-mail aziendali, a siti i cui contenuti non siano legati all'attività lavorativa;
- ad ogni utente e ad ogni ufficio che ne faccia richiesta, viene assegnato uno spazio sui file server centrali; le cartelle presenti nel server sono aree di salvataggio e/o condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi;
- il materiale non pertinente all'attività lavorativa non può essere dislocato, nemmeno

temporaneamente, su personal computer o su cartelle di rete condivise. Il designato IT può procedere in ogni momento alla rimozione di materiale ritenuto non pertinente o potenzialmente pericoloso per la sicurezza del sistema senza preavviso;

- sulle unità di rete condivise vengono svolte regolari attività di back up da parte del designato IT; in caso di perdita dei dati è possibile rivolgersi al designato IT per recuperare i dati mancanti;

7. POTERI DI CONTROLLO DELLA DIREZIONE AZIENDALE

La Società, utilizzando sistemi informativi per esigenze produttive od organizzative (ad esempio per rilevare anomalie o per manutenzione), può avvalersi, nel rispetto dell'art. 4 comma 2 dello Statuto dei Lavoratori, di sistemi che permettano un controllo indiretto a distanza (controllo preterintenzionale) e determinino un trattamento di dati riferiti o riferibili ai lavoratori, nel rispetto delle "Linee guida del Garante per posta elettronica e internet" emesse dall'Autorità Garante per la Protezione dei Dati Personali in data 01/03/2007

A.R.AL. S.p.A. non effettua, in alcun caso, trattamenti di dati personali mediante sistemi informatici che mirino al controllo a distanza dei lavoratori, grazie ai quali sia possibile ricostruire la loro attività e che vengano svolti con i seguenti mezzi:

- lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto tecnicamente necessario per fornire il servizio di posta stesso;
- memorizzazione ed eventuale riproduzione delle pagine web visitate dal dipendente o da soggetti autorizzati;
- lettura e registrazione dei caratteri inseriti dai lavoratori mediante tastiera;
- analisi occulta di computer affidati in uso.

Le attività di controllo, legittimamente svolte dalla Società, ai sensi del presente documento, si attengono in ogni caso ai seguenti principi fondamentali:

1. Necessità, pertinenza e non eccedenza: I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì il principio di pertinenza e non eccedenza. La Società raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti e sono mirate sull'area individuata come "a rischio".

2. Finalità e correttezza: I trattamenti sono effettuati per finalità determinate, esplicite e legittime. Le finalità perseguite dalla Società riguardano o possono riguardare, caso per caso:

- sicurezza sul lavoro,
- sicurezza dei sistemi e relativa risoluzione di problemi tecnici,
- esigenze di organizzazione,
- esigenze di produzione, tecniche o manutentive
- rispetto di obblighi legali,
- tutela della Società.

I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti su dati aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifici audit informatici. In ogni caso non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati-

8. OBBLIGO DI RISPETTO DELLE DISPOSIZIONI: SANZIONI AI DIPENDENTI

È fatto obbligo a tutti i dipendenti e personale autorizzato di osservare le disposizioni portate a conoscenza con il presente regolamento.

Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e risarcitori previsti dai C.C.N.L. applicati, nonché con tutte le azioni civili e penali consentite.

Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, verrà consegnato a ciascun dipendente.

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate.

Schema logico rete Aral