AREUS
Azienda Regionale
Emergenza Urgenza
Sardegna

REGIONE AUTONOMA DELLA SARDEGNA

AREUS – AZIENDA REGIONALE EMERGENZA URGENZA SARDEGNA

REGOLAMENTO SULL'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA INTERNA E DELLA RETE INTERNET

V. 2.0 del 01/03/2022

Premessa

La progressiva diffusione delle nuove tecnologie informatiche ed elettroniche e, in particolare, il libero accesso alla rete Internet di Personal Computer e Smart Phone o altri dispositivi mobili, nonché la delicatezza dei dati trattati dall'AREUS – Azienda Regionale Emergenza Urgenza Sardegna (d'ora in avanti "**AREUS**" o l'"**Ente**"), impone a quest'ultima di adottare un rigoroso regolamento sull'utilizzo della strumentazione informatica ed elettronica aziendale fornita ai dipendenti e ai collaboratori aziendali.

I rischi informatici a cui è esposto l'Ente vengono costantemente individuati e perimetrati anche in considerazione delle maggiori esposizioni conseguenti l'adozione di soluzioni di lavoro cosiddetto "flessibile" o "agile" (d'ora in avanti, per semplicità "**Smart Working**") che consente a dipendenti e collaboratori di lavorare a distanza (anche da casa).

I rischi a cui l'azienda verrebbe esposta, in conseguenza di un non corretto utilizzo della strumentazione informatica fornita al dipendente o al collaboratore, sono di natura patrimoniale e di immagine, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, nonché le responsabilità civili e contrattuali nei confronti di tutti gli stakeholder dell'Ente (in primis, i fruitori dei servizi di soccorso, d'ora in avanti anche gli "**Interessati**").

Poiché l'utilizzo delle risorse informatiche deve comunque ispirarsi ai principi della diligenza e della correttezza, l'Ente ha adottato il presente regolamento interno (d'ora in avanti il "**Regolamento sull'utilizzo della strumentazione informatica interna e della rete internet**" o "**Regolamento**") diretto ad evitare che comportamenti (dolosi o colposi) possano compromettere o minacciare la sicurezza informatica dei sistemi informatici dell'Ente, sia in conseguenza della violazione delle misure di sicurezza interne, sia in conseguenza della violazione di disposizioni di legge e regolamentari conseguenti le norme in materia di tutela dei dati personali o di altre previsioni di legge o disciplinari.

L'insieme delle norme comportamentali ivi incluse è inoltre volto a conformare l'Ente ai princìpi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con la finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano ed eurounitario.

Le previsioni di seguito indicate sono tali da integrare l'eventuale regolamento disciplinare aziendale e la documentazione in materia di sicurezza e di trattamento dei dati predisposta dall'Ente.

Art. 1

Entrata in vigore del Regolamento e pubblicità

Il presente Regolamento entrerà in vigore alla data della sottoscrizione e adozione del medesimo da parte del Direttore Generale dell'Ente. Una copia del Regolamento sarà resa disponibile a ciascun dipendente e collaboratore mediante invio all'indirizzo mail aziendale in uso e/o tramite upload del presente documento digitale su server aziendale in apposita area riservata.

Art. 2

Ambito di applicazione

Il presente Regolamento si applica ad ogni lavoratore o collaboratore assegnatario di beni e risorse informatiche, ovvero utilizzatore di servizi e risorse informative di pertinenza dell'Ente.

Per "**Utilizzatore**" si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, senza distinzione di ruolo o livello, collaboratore (interno o esterno), consulente, fornitore e/o terzo che, anche in modo occasionale, operi all'interno della struttura dell'Ente, utilizzandone beni e servizi informatici.

Art. 3

Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni rientranti nel patrimonio aziendale e sono da considerarsi di esclusiva proprietà dell'Ente.

Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utilizzatore, in base al rapporto in essere, ovvero per scopi professionali afferenti all'attività svolta per l'Ente. In ogni caso, l'utilizzo ha come fine l'esclusivo perseguimento degli obiettivi dell'Ente.

A tal fine, si precisa sin d'ora che tutti i dati e le informazioni trattati per mezzo dei beni e delle risorse informatiche di proprietà dell'Ente, sarà dallo stesso considerato di proprietà dell'Ente stesso e l'Utilizzatore non potrà vantare nei confronti dell'Ente alcun diritto di privativa o riservatezza.

Art. 4

Responsabilità personale dell'Utilizzatore

Ogni Utilizzatore è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ente (di seguito, complessivamente, gli "**Strumenti**"), nonché dei relativi dati trattati per finalità proprie dell'Ente.

A tal fine, ogni Utilizzatore, nel rispetto dei princìpi di diligenza sottesa al rapporto instaurato con l'Ente, è tenuto a tutelare, per quanto di propria competenza, il patrimonio dell'Ente da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo principale consta nella preservazione dell'integrità e della riservatezza dei beni, delle informazioni e delle risorse dell'Ente.

Ogni Utilizzatore, pertanto, è tenuto, in relazione al proprio ruolo ed alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica interna, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza, ovvero violazioni del presente regolamento.

Sono vietati comportamenti che possano arrecare un qualsiasi danno, anche reputazionale o di immagine, all'Ente.

Art. 5

Controlli

L'Ente esclude la configurabilità di forme di controllo interne aventi direttamente ad oggetto l'attività lavorativa dell'Utilizzatore, in linea con quanto prescritto dall'ordinamento giuridico italiano e comunitario (art. 4 della Legge n. 300/1970).

Ciononostante, non si esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro o di tutela del patrimonio aziendale. Per tali evenienze, eventualmente, sarà onere dell'Ente sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali interne ovvero richiedere l'apposita autorizzazione all'Ispettorato del Lavoro, salvo il caso di controllo derivante dall'uso di strumenti adoperati dal lavoratore per rendere la prestazione lavorativa ovvero dall'utilizzo di strumenti di registrazione degli accessi e delle presenze (art. 4, comma 2, Legge 300/1970), nonché ogni altra ipotesi derogatoria prevista dalla normativa vigente.

I controlli eventualmente posti in essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.

I controlli sull'utilizzo da parte dei lavoratori dei beni e dei servizi informatici interni sono in particolare volti a:

1. soddisfare esigenze organizzative aziendali, tra cui: assicurare il coordinamento tra le diverse Aree funzionali nella gestione delle pratiche e dei processi dell'Ente (es. in caso di necessità, l'accesso alla mail aziendale di un dipendente di altra area per verificare l'avvenuta trasmissione di comunicazioni ufficiali dell'Ente); assicurare la continuità delle prestazioni lavorative del dipendente in caso di sua assenza (es. l'accesso alla posta o ai dispositivi aziendali in uso da parte dell'amministrazione di sistema); evitare la duplicazione di attività ed assicurare l'efficienza dei processi aziendali (es., in caso di "lavoro agile", verifica dello

stato di avanzamento di un compito attribuito ad una risorsa, funzionale alla presa in carico del processo da parte di altra risorsa);

2. soddisfare esigenze di tutela del patrimonio aziendale ed in particolare: assicurare la sicurezza e integrità delle reti e dei sistemi informatici aziendali, salvaguardandoli da eventuali aggressioni (interne o esterne) causate da comportamenti dolosi o colposi connessi all'uso degli Strumenti da parte degli Utilizzatori; assicurare l'integrità materiale e l'effettiva operatività degli Strumenti (es. la verifica di una manomissione volontaria o colpevole da parte dell'Utilizzatore di un PC ovvero l'uso non corretto di un software installato nella macchina);
3. soddisfare esigenze di sicurezza sul lavoro, come meglio indicate e dettagliate nell'apposito Documento di Valutazione dei Rischi (DVR) eventualmente adottato dall'Ente o in altro documento adottato in base alla normativa vigente.

L'Ente, riservandosi il diritto di procedere a tali controlli per le esigenze sopra indicate, potrà inoltre utilizzare gli elementi raccolti per tutte le finalità connesse al rapporto di lavoro, ivi incluse quelle relative all'accertamento di inadempimenti contrattuali rilevanti ai sensi dell'art. 2104 c.c. ovvero di illeciti extracontrattuali o disciplinari ascrivibili al dipendente (art. 4, comma 3, Legge n. 300/1970).

I controlli saranno in ogni caso effettuati in base ai principi di proporzionalità, gradualità, e non eccedenza. In attuazione di tali principi:

- in via preliminare l'Ente può provvedere ad eseguire controlli su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree o comunque a un controllo anonimo. In assenza di anomalie ovvero in mancanza di necessità di ulteriori controlli non si effettueranno controlli su base individuale;
- in caso anomalie ovvero di insufficienza dei controlli di cui al punto precedente, l'Ente può procedere a controlli su base individuale o di postazione di lavoro.
- in caso di riscontrato e reiterato uso non conforme delle risorse informatiche l'Area ICT dell'Ente (ai fini del presente Regolamento, l'"**Area Sistemi Informativi**"), che effettua i controlli, segnalerà il comportamento al responsabile dell'area di appartenenza del dipendente, per l'eventuale applicazione delle sanzioni di cui all'art. 17;
- per il personale dirigente il comportamento andrà segnalato alla Direzione dell'Ente e al competente Ufficio per i procedimenti disciplinari per l'adozione degli atti di rispettiva competenza;
- per il personale non dipendente cui non è applicabile il C.C.N.L. il comportamento andrà segnalato alla Direzione aziendale per l'adozione degli atti di specifica competenza.

Ai fini dell'esecuzione dei controlli suddetti, possono essere temporaneamente memorizzate da parte dell'Ente informazioni riguardanti l'accesso e uso dei gestionali interni nonché l'accesso e la navigazione sulla rete Internet e l'uso della posta elettronica aziendale, nonché le ulteriori informazioni necessarie alla verifica di eventuali violazioni della sicurezza interna della rete aziendale, quali:

- data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP assegnato alla macchina;
- data e ora del log-in e del log-off del servizio di posta elettronica sulla base di un determinato fuso orario;
- dati necessari per determinare il tipo di comunicazione;

- informazioni e file di log relativi all'utilizzo della posta elettronica e all'accesso a Internet, che sono tracciate e conservate per finalità organizzative di sicurezza e di controllo da parte dell'azienda per un periodo minimo di una settimana e massimo di sei mesi;
- informazioni e file di log relativi all'uso del gestionale aziendale, anche per il tramite di collegamento in remoto in caso di Smart Working.

Le sopradescritte operazioni di memorizzazione temporanea e/o conservazione dei dati sono di esclusiva competenza del responsabile dell'Area Servizi Informativi. I dati saranno conservati per il tempo strettamente necessario in funzione delle policy di sicurezza aziendali, e comunque non oltre i due anni.

L'accesso ai dati così memorizzati in sede di controllo è consentito ad altri soggetti dell'organizzazione solo su espressa autorizzazione del Direttore Generale o di un suo delegato.

Art. 6

Amministratori di sistema

L'Ente conferisce all'amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche interne. È compito dell'amministratore di sistema:

1. gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ente;
2. gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli Utilizzatori;
3. monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli Utilizzatori, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
4. creare, modificare, rimuovere o utilizzare qualunque account o privilegio, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
5. rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli Utilizzatori, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
6. provvedere alla sicurezza informatica dei sistemi informativi interni, nel rispetto dell'art. 32 del Regolamento UE 2016/679;
7. in conformità a quanto previsto dal precedente art. 5 in materia di controlli per finalità organizzative dell'Ente, utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un Utilizzatore in caso di prolungata assenza, non rintracciabilità o impedimento

dello stesso. Tale attività sarà limitata al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto il suo intervento.

Gli amministratori di sistema sono nominati mediante apposito atto formale adottato dalla Direzione dell'Ente (secondo lo standard specificamente approvato ed allegato al presente Regolamento, **Allegato 1**), contenente la descrizione puntuale dei compiti e delle responsabilità di ciascuna figura. Tale atto varrà anche quale autorizzazione al trattamento dei dati personali ex artt. 2-quaterdecies del D. Lgs. n. 196/2003 e 29 Regolamento UE 2016/679.

L'Ente redige un elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, aggiornato con cadenza annuale ovvero ogni volta che si rilevino modifiche. Nel caso di soggetti esterni incaricati dall'Azienda, anche con compiti di sovrintendere a beni e risorse informatiche interne, questi comunicheranno e aggiorneranno l'elenco degli amministratori di sistema individuati a tale scopo.

Art. 7

Assegnazione degli account e gestione delle password

7.1 – Creazione e Gestione degli Account

L'"**Account Utente**" consente l'autenticazione dell'Utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche interne per ogni singola postazione lavorativa.

1. Gli Account Utente vengono creati dagli amministratori di sistema e sono personali, cioè associati univocamente alla persona assegnataria. Ogni Utilizzatore è responsabile dell'utilizzo del proprio Account Utente.

2. L'accesso al proprio account avviene tramite l'utilizzo delle "**Credenziali di autenticazione**", composte da username e password, comunicate all'Utilizzatore dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.

3. Le Credenziali di autenticazione costituiscono dati interni da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'Ente.

4. Se l'Utilizzatore ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al soggetto gerarchicamente superiore di riferimento.

5. In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità organizzative legate all'attività lavorativa, ovvero per le esigenze produttive interne o per la sicurezza e operatività dei sistemi e delle risorse informatiche dell'Ente, AREUS si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'Utilizzatore per

mezzo dell'intervento dell'amministratore di sistema, in conformità a quanto previsto dall'art. 5 del presente Regolamento.

7.2 – Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle Credenziali di autenticazione da parte dell'amministratore di sistema, l'Utilizzatore ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni 6 mesi e, nel caso di trattamento di categorie particolari di dati personali (art. 9 GDPR) o relativi a condanne penali o reati (art. 10 GDPR), almeno ogni 3 mesi. Decorso tale periodo le credenziali saranno automaticamente disattivate dal sistema.

- L'Utilizzatore, nel definire il valore della password, deve rispettare le seguenti regole:
- Utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, ecc.), di cui almeno uno numerico.
- La password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#$£$%...".
- Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili.
- Evitare l'utilizzo di password comuni o prevedibili.
- Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Scrivere la password su post-it o altri supporti non è conforme alla normativa, compromette in maniera pressoché totale le misure di sicurezza previste, costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

7.3 – Cessazione o modifica degli Account

In caso di interruzione del rapporto di lavoro con l'Utilizzatore, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 30 (trenta) giorni da quella data; entro 90 (novanta) giorni, invece, si disporrà la definitiva e totale cancellazione dell'Account Utente. In caso di variazione delle mansioni o di spostamento di Area dell'Utilizzatore, verranno aggiornate le autorizzazioni associate all'account. A tal fine l'Area competente per la gestione del personale comunicherà tempestivamente i nominativi degli Utilizzatori da cessare o delle variazioni intervenute all'Area dei Sistemi Informativi e Reti Tecnologiche.

Art. 8

Postazioni di lavoro

Per "**Postazione di lavoro**" si intende il complesso unitario di personal computer (di seguito "PC"), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (*device*) concesso in utilizzo all'Utilizzatore. L'assegnatario di tali beni e strumenti informatici interni ha il compito di farne un uso compatibile con i princìpi di diligenza sanciti nell'art. 1176 del Codice Civile.

Tutti i PC e gli altri componenti della Postazione di lavoro sono assegnati personalmente ad una specifica risorsa che ne è responsabile del relativo utilizzo. Ogni Postazione di lavoro è contrassegnata e identificata mediante il nome dell'Utilizzatore assegnatario (iniziale nome seguita dal cognome per esteso).

Ogni PC è dotato di programma "blocca schermo", che si attiva in automatico dopo un breve periodo di attività. Per lo sblocco è necessario l'inserimento della password del relativo Account Utente.

Ogni PC effettua un backup automatico dei dati contenuti nella cartella "Documenti", con cadenza giornaliera, su un apposito storage di rete (NAS) esterno, oppure su disco esterno, anch'esso inventariato, affidato all'Utilizzatore, e munito di cifratura completa.

Tutti i componenti della Postazione di lavoro di proprietà dell'Ente sono inventariati, tracciati e suddivisi in base alle rispettive Postazioni di lavoro in apposito documento ("**Inventario Hardware**") che si allega al presente Regolamento per farne parte integrante e sostanziale (**Allegato 2**). L'Inventario hardware sarà oggetto di aggiornamento e verifica periodica con cadenza semestrale.

Al fine di disciplinare un corretto utilizzo di tali beni l'Ente ha adottato le seguenti regole tecniche:

- Ogni PC, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (*device*), sia esso acquistato, noleggiato o affidato in locazione, è uno strumento di lavoro ed è concesso all'Utilizzatore per lo svolgimento in via esclusiva delle proprie mansioni lavorative e comunque per finalità strettamente attinenti all'attività svolta.
- È dovere di ogni Utilizzatore usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente.
- Il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita è necessario presentare espressa richiesta scritta al proprio responsabile di riferimento, il quale ne valuterà i requisiti tecnici, l'aderenza alle policies interne e al ruolo ricoperto all'interno dell'Ente.
- Le Postazioni di lavoro non devono essere lasciate incustodite con le sessioni utente attive.
- Quando un Utilizzatore si allontana dalla propria Postazione di lavoro deve bloccare tastiera e schermo del PC con l'apposito programma blocca schermo (anche detto *screensaver*) o effettuare il log-out dalla sessione.

- L'Utilizzatore deve segnalare con la massima tempestività all'amministratore di sistema o al proprio responsabile di Area eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici interni a soggetti terzi.
- L'Ente si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'Utilizzatore quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non possono essere collegati ai PC o alle reti informatiche interne dell'Ente, salvo preventiva autorizzazione scritta da parte della Direzione generale o di un suo delegato.

Resta inteso che tutti i beni e la strumentazione informatica oggetto del presente Regolamento, costituenti la Postazione di lavoro, rimangono di esclusiva proprietà e dominio dell'Ente, che in conseguenza dei rapporti instaurati con gli Utilizzatori ne disciplina l'assegnazione o la relativa revoca.

Art. 9

Dispositivi (*devices*): PC Desktop, Laptop, Tablet, Smartphone, etc.

Per l'espletamento delle proprie mansioni per il tramite della Postazione di lavoro gli Utilizzatori sono inoltre tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio dispositivo (*device*), se non previa esplicita autorizzazione dell'Ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni) che la esegue per mezzo dell'amministratore del sistema;
- Non è consentito rimuovere, danneggiare o asportare componenti hardware;
- Non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'Ente;
- È onere dell'Utilizzatore, in relazione alle sue competenze lavorative, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
- È onere dell'Utilizzatore spegnere il proprio PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'Utilizzatore ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della loro riconsegna;

- Non è consentito all'Utilizzatore caricare o inserire all'interno del PC o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, l'Ente, con l'intervento degli amministratori di sistema, cancellerà tutti i dati presenti in modo sicuro (es. formattazione completa dei dischi non in modalità veloce) prima di destinare i computer ad usi diversi ed in ogni caso quando i dati non sono più necessari per le attività a cui si è preposti ovvero prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

Art. 10

Software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli Utilizzatori dovranno ottenere espressa autorizzazione dell'Ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni) per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio *freeware* o *shareware*.

Gli Utilizzatori sono tenuti a far uso della Postazione di lavoro mediante il solo software autorizzato dall'Ente, come inventariato e classificato nell'apposito Inventario Software che si allega al presente Regolamento per farne parte integrante e sostanziale (**Allegato 3**).

Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun Utilizzatore è tenuto a osservare per un corretto utilizzo del software all'interno dell'Ente:

- Le licenze d'uso del software sono acquistate da vari fornitori esterni. L'Utilizzatore è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli Utilizzatori sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza.
- Non è consentito eseguire il download o l'upload di software non autorizzato.
- Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.
- La duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

ART 11

Dispositivi mobili di connessione (internet key)

Agli Utilizzatori può essere concessa in dotazione anche una chiavetta o dispositivo per la connessione alla rete dell'Ente per consentire lo svolgimento delle mansioni lavorative anche da remoto.

I suddetti dispositivi mobili di connessione devono essere utilizzati esclusivamente sui dispositivi forniti in dotazione dall'Ente e non è consentito concederne l'utilizzo a soggetti terzi né utilizzarli su altri computer sia personali che di terzi.

Le specifiche relative ai limiti entro cui l'Utilizzatore potrà utilizzare il servizio offerto tramite il dispositivo sono comunicate nella fase di consegna dell'apparato.

L'Utilizzatore dovrà attenersi ai suddetti limiti; in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

Art. 12

Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.

L'utilizzo di tali supporti risponde alle direttive di seguito riportate:

- non è consentito utilizzare supporti rimovibili, se non preventivamente autorizzati per iscritto dall'Ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni);
- è onere dell'Utilizzatore custodire i dispositivi di memoria contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto; il contenuto di tali dispositivi deve essere cifrato o protetto tramite password.
- Se autorizzati in base alle procedure previste, una volta connessi all'infrastruttura informatica dell'Ente, i dispositivi saranno soggetti (ove ciò sia compatibile) al presente Regolamento.

Art. 13

Stampanti, fotocopiatrici e fax

L'utilizzo di tali strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Ente.

Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa, è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Gli strumenti dotati di memoria, connessi o meno in rete, sono gestiti dall'Amministratore di Sistema che provvede alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

Art. 14

Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione del singolo Utilizzatore, l'Ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile. Si richiamano, in proposito, le previsioni riportate nel regolamento adottato con Deliberazione D.G. n. 240 del 07/10/2019.

Le specifiche relative ai limiti entro cui l'Utilizzatore potrà utilizzare tali strumenti sono comunicate nella fase di consegna del dispositivo. L'Utilizzatore dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

Come per qualsiasi altra dotazione interna facente parte della Postazione di lavoro, il dispositivo mobile rappresenta un bene dell'Ente concesso in uso per scopi esclusivamente lavorativi.

Al fine di controllo del corretto utilizzo dei servizi di telefonia interna, l'Ente può esercitare i diritti di cui all'art. 124 del D. Lgs. 196/2003, rubricato "*fatturazione dettagliata*" richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.

Eventuali controlli saranno eseguiti secondo criteri, modalità e limiti descritti all'art. 5 del presente Regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'Utilizzatore per il periodo interessato.

L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

a) Ciascun Utilizzatore assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione;

b) I dispositivi devono essere dotati di password di sicurezza, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che:

   - il codice PIN dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione;
   - il codice PIN o altri codici di accesso dovranno essere modificato dall'assegnatario con cadenza al massimo semestrale;
   - ogni Utilizzatore deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'Ente.

c) In caso di furto, danneggiamento o smarrimento del dispositivo mobile l'Utilizzatore assegnatario dovrà darne immediato avviso all'Ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'Utilizzatore stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;

d) In caso di furto o smarrimento l'Ente si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;

e) Non è consentito all'Utilizzatore caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare o almeno ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione;

f) Non è consentito all'Utilizzatore effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano preventivamente autorizzate dall'Ente;

g) L'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'Utilizzatore le responsabilità derivanti dall'installazione non autorizzata che costituisce violazione del presente regolamento;

h) Salvo diversi specifici accordi derivanti da esigenze di servizio, al momento della consegna di tablet o smartphone l'Utilizzatore è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che in caso contrario l'Ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

Art. 15

Gestione utilizzo della rete internet

Ciascun Utilizzatore potrà essere abilitato alla navigazione Internet e pertanto si richiamano tutti gli Utilizzatori a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'Ente.

La connessione a Internet, in quanto strumento a disposizione degli Utilizzatori per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a) L'utilizzo è consentito esclusivamente per scopi interni e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.

b) Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'Ente.

c) È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

d) Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames).

e) Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica.

f) È consentito l'utilizzo di soluzioni di Instant Messenger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'Ente.

g) Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.

h) Non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro.

i) Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente approvata.

j) È severamente vietato eseguire o favorire pratiche di spamming.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'Ente.

Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole l'Ente si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

Art. 16

Gestione e utilizzo della posta elettronica aziendale

16.1 – Principi Guida

Per ciascun Utilizzatore titolare di un Account Utente, l'Ente provvede ad assegnare una casella di posta elettronica individuale così composta:

nome.cognome@areus.sardegna.it

I servizi di posta elettronica devono essere utilizzati esclusivamente a scopo professionale: l'account e-mail è uno strumento di proprietà dell'Ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate. È fatto espresso divieto all'Utilizzatore di far uso della casella postale assegnata dall'Ente per fini privati e personali.

Ad uno stesso Utilizzatore possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri Utilizzatori dello stesso gruppo/ufficio/dipartimento. Tali caselle di posta elettronica devono essere utilizzate esclusivamente per la ricezione dei messaggi mentre per le risposte o gli invii deve sempre essere utilizzata la casella personale.

Attraverso le caselle e-mail interne, gli Utilizzatori rappresentano pubblicamente l'Ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine dell'Ente.

Gli Utilizzatori sono responsabili del corretto utilizzo delle caselle di posta elettronica interna, conformemente alle presenti regole. In particolare, gli stessi devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
- evitare di aprire messaggi di posta in arrivo con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif e ogni altra

estensione non riconosciuta. È necessario porre molta attenzione, inoltre, ai link contenuti nel messaggio e alla credibilità del messaggio e del mittente, anche se conosciuto, per evitare casi di phishing o frodi informatiche;

- inviare preferibilmente files in formato PDF firmato digitalmente;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
- rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.

Inoltre, non è consentito agli Utilizzatori:

a) diffondere il proprio indirizzo e-mail interna attraverso la rete internet;

b) utilizzare la casella di posta elettronica interna per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente, per esempio presentazioni o materiali video interni;

c) prendere visione della posta altrui, salvo i casi previsti e regolamentati dall'Azienda.

d) modificare la configurazione hardware e software della propria macchina o utilizzare sistemi client di posta elettronica non conformi a quelli accettati dall'azienda;

e) inviare messaggi di posta elettronica in broadcast a tutti gli Utilizzatori dell'azienda se non per comunicazioni di interesse generale attinenti alle mansioni assegnate alla propria Area;

f) diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione;

Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli Utilizzatori di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale". Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per telefono) e mai assieme ai dati criptati.

L'invio di e-mail a destinatari multipli deve essere effettuato avendo bene a mente che la divulgazione di un indirizzo di posta elettronica rappresenta, se non autorizzato, una violazione del della vigente normativa in ambito privacy. L'indirizzo di posta elettronica di un individuo, infatti, costituisce un dato personale ai sensi dell'art. 4, comma 1, n. 1), GPDR, e pertanto non può essere divulgato senza previo consenso del suo titolare. Nei casi di invio di e-mail a più destinatari gli Utilizzatori devono assicurarsi che gli indirizzi e-mail dei destinatari in chiaro siano compatibili con il rispetto della

normativa sulla privacy. Di conseguenza, gli stessi sono tenuti verificare se occorra usare il Cc o il Ccn a seconda del contesto di spedizione delle e-mail a soggetti multipli.

Occorre infine che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.

Le caselle di posta elettronica certificata saranno di norma associate al protocollo informatico. Il titolare della casella di posta elettronica certificata ha l'obbligo di presidiare la stessa, verificando periodicamente il suo contenuto. Nei casi in cui l'Ente si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

16.2 – Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun Utilizzatore, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano di inviare automaticamente messaggi di risposta contenenti le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

In caso di assenze non programmate, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'Ente disporrà, lecitamente e mediante personale appositamente incaricato (l'Amministratore di Sistema oppure un suo incaricato), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.

Nel caso in cui l'Ente necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'Utilizzatore resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario" (di norma il Responsabile dell'Area di appartenenza), da intendersi quale lavoratore previamente autorizzato al trattamento per iscritto dall'Utilizzatore assente;
- di tale attività sarà redatto apposito verbale e informato l'Utilizzatore interessato alla prima occasione utile.

16.3 – Cessazione dell'indirizzo di Posta Elettronica aziendale

In caso di interruzione del rapporto di lavoro con l'Utilizzatore, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. A tal fine l'Area del Personale comunicherà tempestivamente i nominativi degli Utilizzatori da cessare all'Area dei Sistemi Informativi e Reti Tecnologiche. In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti e necessari per l'esercizio delle proprie attività, nei limiti della minimizzazione del

trattamento e comunque non oltre i termini di conservazione specificamente dalla normativa nazionale o comunitaria vigente.

Art. 17

Sanzioni

La violazione di quanto previsto dal presente Regolamento, rilevante anche ai fini contrattuali ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori), nonché in conformità alle previsioni dell'apposito regolamento disciplinare dell'Ente, ove esistente.

Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'Ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici interni.

In caso di violazione accertata delle regole e degli obblighi esposti in questo Regolamento da parte degli Utilizzatori, AREUS si riserva la facoltà di sospendere, bloccare o limitare gli Account Utente, quando ciò appaia ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei beni e delle risorse informatiche dell'Ente, ovvero per impedire la reiterazione della violazione.

Art. 18

Informativa agli Utilizzatori ex art. 13 Regolamento (UE) 2016/679

Il presente Regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici interni e relativamente al trattamento di dati personali svolti dall'Ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'art. 5 del Regolamento, vale quale informativa specifica ai sensi dell'art. 13 del Regolamento (UE) 2016/679 nonché dell'art. 4, comma 3, L. 300/1970.

Art. 19

Comunicazioni

Contestualmente all'assegnazione di un Account Utente il presente Regolamento è messo a disposizione degli Utilizzatori per la relativa consultazione. La versione più aggiornata dello stesso è pubblicata sia in formato immateriale digitale nell'apposita pagina del sito internet dell'Ente ovvero, ove esistente, nel cloud aziendale, sia in formato fisico cartaceo allo scopo di facilitarne la diffusione presso tutti gli interessati.

Per ogni aggiornamento del presente Regolamento o dei relativi allegati sarà data comunicazione sulle bacheche interne e tramite l'invio di specifico messaggio e-mail a tutti gli Utilizzatori, che sono tenuti a conformarsi alla versione più aggiornata.

Le richieste di autorizzazione o concessione previste dal presente regolamento possono essere inoltrate all'Ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

Art. 20

Approvazione del Regolamento

Il presente Regolamento è approvato e adottato dalla Direzione Generale dell'Ente con Deliberazione D.G. n. XX del xx/xx/2022 e sarà sottoposto, ove richiesto per legge, ad apposito accordo con le competenti rappresentanze sindacali ovvero all'autorizzazione preventiva dell'Ispettorato del lavoro, in ottemperanza di quanto previsto dall'art. 4 della Legge n. 300/1970.

Allegati:

1. Standard nomina di amministratore di sistema
2. Inventario Hardware AREUS
3. Inventario Software AREUS