Regolamento per l'utilizzo delle risorse informatiche e telematiche di ARPACAL

Redatto: U.O. Sistemi Informativi Sicurezza e Privacy		**Firma** _____
Revisione: 2.0	**Data:** 27 Maggio 2013	**Firma** _____
Approvato: Direzione Generale (Titolare)	**Data:**	**Firma** _____
Approvato: Direzione Scientifica (Titolare)	**Data:**	**Firma** _____
Approvato: Direzione Amministrativa (Titolare)	**Data:**	**Firma** _____
Inviato alla RSU: SI __ NO __	**Data:** **Prot.:**	
Inviato alle OO.SS.: SI __ NO __	**Data:** **Prot.:**	


Privacy


http://www


OpenOffice.org
the free and open productivity suite


Microsoft
Office


WEB

INDICE

PARTE PRIMA

Finalità del Regolamento

L'utilizzo delle risorse informatiche e telematiche della ARPACAL deve sempre ispirarsi al principio della diligenza e della correttezza, criteri normalmente già adottati nell'ambito di un qualsiasi rapporto di lavoro ed in particolare in quello pubblico.

Il presente regolamento interno ha lo scopo di identificare alcuni comportamenti che possono evitare o creare problemi per la sicurezza del trattamento dei dati informatici all'interno di ARPACAL, esponendo l'Agenzia sia a conseguenze di carattere penale che a danni di tipo patrimoniale.

In merito a quest'ultimo punto, si ricorda, fra l'altro, che le risorse hardware e software messe a disposizione dalla ARPACAL appartengono al patrimonio di ARPACAL stessa **e sono solo in assegnazione alla singola risorsa umana**.

Vista la distribuzione dell'organizzazione sul territorio regionale e considerato che il Sistema Informatico di ARPACAL è in corso di evoluzione, ai fini del rispetto del D.Lgs. 196/2003 e s.m.i. (c.d. Codice Privacy), l'ARPACAL intende adottare un modello funzionale che possa meglio rispondere ai bisogni degli utenti, sia se risorse umane in forza alle Direzioni Centrali e sia se in forza ad un qualsiasi Dipartimento Provinciale, Centro di Eccellenza, Centro Funzionale Strategico od Unità Organizzativa.

Il presente Regolamento è quindi, in sintesi, volto a:

a) assicurare il rispetto della legislazione vigente in materia di utilizzo delle risorse informatiche e telematiche di ARPACAL, perseguendo altresì la massima efficienza ed efficacia nell'utilizzo delle stesse;

b) tutelare al meglio la riservatezza delle informazioni e dei dati;

c) garantire il principio di necessità nell'utilizzo dei sistemi informatici e dei programmi informatici di cui all'art. 3 del D.Lgs. n. 196 del 2003 e s.m.i. (Codice in materia di protezione dei dati personali, d'ora in poi **Codice** per il fine del presente Regolamento), al fine di ridurre al minimo l'utilizzazione di dati personali e di dati identificativi degli **interessati**; garantire altresì il principio di correttezza di cui all'art. 11 del medesimo D.Lgs. n. 196 del 2003 e s.m.i., secondo il quale le caratteristiche essenziali dei trattamenti devono essere note ai lavoratori;

d) impedire che gli utenti, utilizzando le risorse informatiche e telematiche di ARPACAL, compiano abusi legati all'impiego improprio delle risorse della rete Intranet ed Internet.

Ambito di applicazione, definizioni, destinatari

Al fine dell'applicazione del presente regolamento si considerano:

- per **utente** qualsiasi soggetto che a qualunque scopo sia autorizzato ad accedere alle risorse informatiche e telematiche di ARPACAL quali, in maniera non esaustiva ma meramente esemplificativa, Direttori, Dirigenti, Personale del Comparto, Consulenti, Stagisti, Tirocinanti ed eventuali altri Collaboratori dell'Agenzia in generale;

- per **risorse informatiche e telematiche** qualsiasi tipo di hardware, computer, mezzo di comunicazione elettronica, rete di trasmissione dati, modem, stampante, scanner, apparecchiatura per l'archiviazione elettronica dei dati con i relativi supporti di memorizzazione, video terminale, software operativo e programma applicativo, dato e informazione di formato elettronico di proprietà e, comunque, in disponibilità di ARPACAL;

- per **amministratori di sistema (centrali e periferici)** le persone fisiche dedicate alla gestione e alla manutenzione di impianti di elaborazione o di componenti di questi e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche di apparati di sicurezza e di sistemi software complessi, nella misura in cui consentano di intervenire su dati personali; soggetti che pur non essendo preposti ordinariamente a operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni) possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi applicative comportanti elevate criticità rispetto alla protezione dei dati personali; gli amministratori di sistema saranno riportati sul **Documento Programmatico della Sicurezza (DPS)** sulla base delle designazioni formali ricevute o effettivamente esercitate (es. Amministratore del portale web istituzionale, Amministratore dell'Albo Pretorio online, etc.); esclusivamente dal punto di vista delle attività svolte ai fini della sicurezza informatica e telematica fanno riferimento alla U.O. Sistemi Informativi e Privacy; hanno l'obbligo di operare secondo le regole stabilite e concordate con la U.O. Sistemi Informativi Sicurezza e Privacy ed hanno l'obbligo di non divulgare informazioni tecniche agli utenti che potrebbero causare problemi durante l'uso del Sistema Informatico di ARPACAL. In caso di supporto remoto da parte di Enti e Società esterne, in particolare per la manutenzione evolutiva e correttiva delle applicazioni informatiche a qualsiasi titolo censite ed utilizzate da ARPACAL, tali Enti e Società esterne dovranno comunicare i dati identificativi dell'**Amministratore di sistema (esterno)** autorizzato ad operare come supporto remoto, ai fini dell'obbligo di iscrizione nell'apposita sezione del DPS;

- per **custodi delle password**, le persone fisiche con l'incarico di custodire le password per l'accesso in rete ed ai dati da parte degli utenti incaricati, tenere il registro degli incaricati che hanno effettivamente consegnato le password e segnalare a coloro che non lo hanno fatto la necessità di effettuazione di deposito password (in busta chiusa) nonché collaborare con l'Amministratore di sistema per far revocare e far registrare quelle non utilizzate per un periodo superiore a tre mesi.

I criteri e le norme del presente Regolamento trovano applicazione nei confronti di qualsiasi soggetto, di seguito denominato **utente**, che a qualunque scopo sia autorizzato ad accedere alle risorse informatiche e telematiche di ARPACAL.

PARTE SECONDA

Credenziali di autenticazione

L'accesso delle stazioni di lavoro di ARPACAL in rete sarà protetto (Art. 34 ed All. B del Codice) da credenziali di autenticazione, formate da un codice per l'identificazione dell'**utente incaricato** (username) e da una parola chiave riservata (password) conosciuta solamente dall'utente incaricato. L'assegnatario dovrà custodire le proprie credenziali con la massima diligenza al fine di mantenerne l'assoluta segretezza, essendo proprio l'esclusività della conoscenza il criterio che consente il suo univoco riconoscimento da parte del sistema. La progettazione del sistema per il rilascio e la gestione automatica delle credenziali di autenticazione è in fase avanzata, trattandosi di scelte tecniche che dipendono anche dall'architettura di rete, su scala regionale, che realmente sarà disponibile, essendo soggetta a potenziali restrizioni contrattuali con fornitori di servizi per i collegamenti in trasmissione dati tra le sedi ed ottimizzazioni, a causa di problemi legati alle risorse di Bilancio di ARPACAL ed effettivamente disponibili per i noti problemi di "spending review".

Assegnazione delle credenziali

Le assegnazioni delle credenziali di accesso alle risorse informatiche dovranno essere richieste secondo le modalità di seguito indicate:

- l'**utente interno** (colui o colei che intrattiene un rapporto di lavoro stabile con ARPACAL) che intende avere accesso ai software di gestione, alle reti Intranet ed Internet di ARPACAL deve richiedere l'assegnazione di credenziali di acceso mediante presentazione di apposita istanza alla U.O. Sistemi Informativi Sicurezza e Privacy autorizzata dal Direttore/Dirigente a cui la risorsa funzionalmente risponde, ai fini del necessario censimento anagrafico di natura informatica;

- le richieste di abilitazione **per personale esterno** (collaboratori, stagisti, tirocinanti, ed eventuali ospiti) dovranno essere parimenti richieste ed autorizzate, a seconda della struttura organizzativa di afferenza, dai Direttori/Dirigenti delle Direzioni Centrali, dei Dipartimenti Provinciali, dei Centri e delle U.O. di ARPACAL; ovviamente le credenziali rilasciate avranno una durata limitata all'effettiva durata dell'attività di tale personale e scadranno automaticamente dopo tre mesi dal loro ultimo utilizzo.

Ad un utente, oltre alle credenziali di accesso per l'utilizzo in rete della stazione di lavoro (pc e/o notebook assegnato), possono essere attribuite ulteriori credenziali di autenticazione, a seconda della risorsa e/o del servizio da proteggere, per esempio:

- elaboratore assegnato all'utente; per tale elaboratore esisteranno più account d'uso, di cui uno dedicato agli amministratori di sistema per le attività di supporto da locale e da remoto, per l'installazione autorizzata di nuovi programmi e per qualsiasi manutenzione necessaria della stazione di lavoro; si precisa che a tutti gli utenti che intendono utilizzare risorse in rete di ARPACAL saranno assegnati, ai fini della sicurezza, privilegi "standard"; eccezioni formalmente richieste ed autorizzate dalla U.O. Sistemi Informativi Sicurezza e Privacy potranno riguardare esclusivamente gli stessi amministratori di sistema o sistemi in funzionamento stand-alone;
- servizi di rete (e-mail, aree condivise, etc.);
- eventuale accesso Intranet;
- eventuale accesso Internet;
- accesso a programmi applicativi residenti sui server di ARPACAL.

Aggiornamento delle credenziali

Il sistema di autenticazione controllerà che l'utente, autorizzato all'uso di risorse in rete locale di ARPACAL, ricevute le credenziali di accesso, provveda a modificare autonomamente la propria password principale, con la seguente tempistica:

- immediatamente, non appena la riceve per la prima volta;
- successivamente, almeno ogni tre mesi.

Le regole base per la generazione della password sono le seguenti:

- deve essere composta da almeno otto caratteri;
- deve essere formata da lettere (maiuscole o minuscole), numeri e caratteri di interpunzione.

Il rispetto della qualità delle password sarà normalmente garantito e controllato automaticamente dal sistema informatico di autenticazione.

Consegna delle credenziali

L'utente, autorizzato all'uso di risorse informatiche e telematiche di ARPACAL, ricevute le credenziali principali ed opportunamente modificate, deve provvedere a consegnare in busta chiusa le stesse al **custode delle password** competente per la propria struttura di appartenenza.

Uso delle stazioni di lavoro

Non è consentito installare autonomamente programmi provenienti dall'esterno (o da qualsiasi) altra fonte, in particolare di tipo files eseguibili, senza l'autorizzazione esplicita della U.O. Sistemi Informativi Sicurezza e Privacy, né è consentito utilizzare programmi diversi da quelli acquistati, installati o autorizzati ufficialmente da ARPACAL. E' vietato attivare condivisione in rete dei propri dischi, o di aree di questi dedicate a directories e files. E' inoltre vietata la copiatura di files eseguibili, giochi sia sui dischi di rete che sui dischi locali delle proprie stazioni di lavoro assegnate da ARPACAL.

I rischi derivanti dall'inosservanza di tale disposizione possono i seguenti:

- introduzione di virus informatici, "cavalli di troia" ed altri programmi "maliziosi";
- compromissione della stabilità delle applicazioni già installate con dispendio di tempo, risorse e rischio di perdita dati;
- sovraccarico della rete locale, con degrado delle prestazioni per altri utenti connessi in rete;
- sovraccarico dei collegamenti su rete Internet, con degrado delle prestazioni per altri utenti;
- violazione della normativa a tutela dei diritti d'autore (D. Lgs. 518/92 e L. 248/2000) che impone l'utilizzo o di software libero o di software proprietario munito di regolare licenza.

L'utente, creato con account limitato, non può modificare le impostazioni dell'elaboratore, mentre nell'eventuale caso di utenti che nel periodo transitorio di applicazione di tale regolamento risultassero ancora autorizzati con account non limitati, risulta comunque vietata la modifica delle impostazioni assegnate senza l'autorizzazione esplicita della U.O. Sistemi Informativi Sicurezza e Privacy in quanto trattasi di funzionalità che a regime saranno configurabili solo e comunque dall'amministratore di sistema (es. particolare impostazione della configurazione TCP/IP per l'accesso in rete, configurazione per la fruibilità di aggiornamenti di software di sistema, di software di sottosistema o di software applicativo, configurazione link per gli accessi alle applicazioni, risoluzione dello schermo impostata, impostazione di password di bios all'atto di accensione della macchina).

A tutti gli utenti è espressamente vietato e costituisce addebito contestabile a fini disciplinari **l'uso di software e hardware atto ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e documenti informatici o durante le sessioni di lavoro in rete (es. in conseguenza di attività di sniffer, di spoofing, di creazione di hot spot wi-fi, etc.).**

Non è consentita l'installazione sul proprio elaboratore di alcun dispositivo di memorizzazione esterna e/o comunicazione di tipo hard disk o modem esterno senza l'autorizzazione esplicita della U.O. Sistemi Informativi Sicurezza e Privacy. L'uso di USB-pen e similari è condotto sotto la personale responsabilità dell'utente e solo ovviamente per uso istituzionale.

Ogni utente deve prestare la massima attenzione durante l'uso di supporti provenienti dall'esterno, autorizzato comunque solo nel caso di contenuto preventivamente noto (floppies, CD, DVD, memorie USB sicure o similari), avvertendo immediatamente l'amministratore di sistema di riferimento (centrale o periferico) nel caso in cui vengano rilevati virus o malware.

Gli amministratori di sistema (centrale e periferici), nell'ambito delle proprie attribuzioni legate alla sicurezza e alla manutenzione informatica, avranno la facoltà di accedere in qualunque momento da remoto o direttamente da locale (dopo avere informato preventivamente l'utente interessato) alla stazione di lavoro dell'utente.

L'elaboratore assegnato deve essere spento al termine del turno di lavoro od anche nel caso di assenze prolungate dall'ufficio. Lasciare un elaboratore acceso ed incustodito può consentire accessi impropri da parte di terzi senza che vi sia la possibilità di provarne in seguito un eventuale indebito uso.

Per nessun motivo la postazione di lavoro assegnata all'utente può essere aperta e manipolata, nè nel caso di presunto guasto hardware nè per qualsiasi altra motivazione. L'apertura, la manipolazione, la sottrazione di parti di essa (hard disk, memoria RAM, schede, etc.) è segnalato da parte dell'amministratore di sistema (centrale o periferico) al Direttore/Dirigente a cui la risorsa è assegnata, ai fini della contestazione dell'addebito e del conseguente potenziale procedimento disciplinare. La responsabilità della postazione di lavoro ricade sempre sull'assegnatario della stessa.

Aree di lavoro condivise

La U.O. Sistemi Informativi Sicurezza e Privacy, sulla base dell'analisi dei bisogni trasmessi dalle Direzioni Centrali e Dipartimentali cercherà, compatibilmente con le risorse di Bilancio messe effettivamente a disposizione della stessa, di elevare la qualità e la quantità di applicazioni informatiche da rendere effettivamente disponibili agli utenti, per "traghettare" l'Agenzia da un

modello funzionale che vede un eccessivo uso di software di produttività individuale, ad uno più idoneo tipico delle organizzazioni evolute, con la tenuta di applicazioni e banche dati centralizzate a fini di elevare il knowledge management ed il decision support agenziale a tutti i livelli. In tale fase transitoria, sui server di ARPACAL, custoditi presso i locali del Centro Elaborazione Dati (CED) di Catanzaro Lido ma eventualmente anche su altri server di sedi periferiche, la U.O. Sistemi Informativi Sicurezza e Privacy renderà disponibili aree di memorizzazione per custodire directories e files contenenti informazioni strettamente correlate all'attività lavorativa (qualunque altro tipo di file non può essere allocato, nemmeno per brevi periodi, su tali aree, se non previa espressa autiorizzazione). Le finalità principali di tale servizio sono le seguenti:

- condivisione delle informazioni fra più utilizzatori;
- consentire ad un singolo utente di disporre di una propria area personale, riservata e centralizzata su cui archiviare i propri files di lavoro, evitando la duplicazione dei dati (per esempio su elaboratore locale e server) situazione che, oltre ad occupare inutilmente risorse, rende più complicata la tutela della sicurezza e quindi della privacy;
- possibilità di effettuazione di sistematici backup in maniera trasparente all'utilizzatore.

La U.O. Sistemi Informativi Sicurezza e Privacy può in qualunque momento procedere alla rimozione di files o applicazioni che dovessero risultare pericolosi per la sicurezza della rete e del Sistema Informatico, previa informazione ad eventuali utenti ed utilizzatori interessati.

E' buona regola che gli utenti effettuino una periodica pulizia delle aree di memorizzazione mediante la cancellazione di directories e files non più necessari, anche ai fini delle prestazioni della propria postazione di lavoro con alta probabilità di degrado delle stesse.

Le stampe cartacee (dati, tabelle, riepiloghi, documenti, etc.) devono essere effettuate, sulla base della disposizione del Commissario Straordinario Prot. 819 del 18/01/2012, solo se strettamente necessarie alle attività operative. Esse devono essere ritirate prontamente dall'utilizzatore evitando di lasciarle giacere nel vassoio della stampante (locale o condivisa), dove potrebbero essere visionate e/o prelevate da persone non autorizzate.

Utilizzo dei supporti riutilizzabili

L'uso di supporti riutilizzabili (magnetici e non) quali dischetti, dischi riscrivibili, memorie, etc., con particolare riguardo a quelli contenenti dati sensibili e giudiziari, non sarà necessario se l'utente avrà cura di memorizzare le informazioni sulle aree di sistema soggette a periodico backup. Nel caso ciò fosse inevitabile, l'utente informerà l'amministratore di sistema di tale circostanza, fermo restando che dovrà custodire ed utilizzare gli stessi supporti in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti. In particolare:

• durante il loro utilizzo essi devono essere conservati con scrupolo e precauzione (per esempio in cassetti o armadietti chiusi a chiave);

• quando cessa lo scopo per cui i dati sono stati memorizzati, i supporti non possono venire semplicemente abbandonati, ma si deve rendere il loro contenuto inintellegibile e non ricostruibile tecnicamente. A tal fine la semplice cancellazione non è una misura sufficiente: bisognerà riformattare in modo completo (e non veloce) i supporti stessi, fermo restando che solo mediante appositi software è possibile prevenire all'eliminazione definitiva dei dati (eventualmente, nel caso degli hard disk, mediante una formattazione a basso livello)

Utilizzo di PC portatili (notebook e similari) di ARPACAL

L'utente è responsabile del notebook o apparecchiatura portatile assegnata da ARPACAL: deve usarlo e custodirlo con diligenza sia all'esterno (convegni, visite aziendali, presentazioni) che all'interno della sede di lavoro, nonché durante gli spostamenti.

Ai notebook ed altre apparecchiature portatili si applicano tutte le regole di utilizzo già descritte per gli elaboratori assegnati da ARPACAL. In più deve essere prestata attenzione alla rimozione di eventuali files elaborati sullo stesso prima della riconsegna alla U.O. Sistemi Informativi Sicurezza e Privacy o al Direttore/Dirigente della struttura di appartenenza.

PARTE TERZA

Uso della rete Internet e dei relativi servizi

L'elaboratore abilitato alla navigazione in Internet costituisce uno strumento messo a disposizione di ARPACAL per supportare lo svolgimento della propria attività lavorativa ed è quindi vietata la navigazione in Internet per finalità differenti. Tale attività sarà tecnicamente implementata ed incrementata mediante l'uso di sistemi di tipo firewall sia di tipo software che hardware.

Non è consentito agli utenti scaricare da Internet software di qualsiasi tipo (freeware, shareware, aggiornamenti) né files multimediali (musica, filmati, immagini), né collegarsi a siti che effettuano streaming audio e/ o video (per esempio ascolto in tempo reale di una radio o di una tv tramite Internet). Tali attività, oltre a costituire una fonte di potenziali pericoli per la sicurezza del sistema ed un'eventuale violazione dei diritti d'autore, sovraccaricano notevolmente la rete degradandone le prestazioni e facendo lievitare significativamente i bisogni ed i costi per la trasmissione dati. Tuttavia, qualora dovesse verificarsi la necessità di avere a disposizione un documento elettronico di dimensioni significative ed utile a più persone nell'ambito di ARPACAL, si potrà richiederne il download alla U.O. Sistemi Informativi Sicurezza e Privacy che provvederà ad effettuarlo una tantum attraverso la rete Internet esterna ed a renderlo poi disponibile a tutti gli interessati mediante download interno attraverso la rete Intranet della ARPACAL (operazione che può essere ripetuta più volte senza nuovamente generare traffico esterno con il gestore della rete di telecomunicazioni).

È vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi esplicitamente autorizzati per lo svolgimento dell'attività lavorativa.

Non è consentita alcuna forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

Non è consentita la partecipazione a forum non inerenti l'attività lavorativa, l'utilizzo di social network, chat line, di bacheche elettroniche e registrazioni in guest books.

Per evitare pericoli di diffusione di virus informatici e rischi di sovraccaricamento della rete non sono quindi consentiti:

- la navigazione per motivi diversi rispetto a quelli funzionali all'attività lavorativa;
- l'upload di software di qualunque tipo (freeware e shareware) da siti Internet, se non espressamente autorizzato dalla U.O. Sistemi Informativi Sicurezza e Privacy .

A tal fine ARPACAL può adottare misure di tipo tecnologico:

- individuando categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
- il trattamento di dati che seppur estratti in modalità aggregata e tali da precludere l'immediata identificazione degli utenti forniscano informazioni di controllo utili agli amministratori di sistema;
- la conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza.

Non è consentito altresì:

- acquisire e diffondere prodotti informativi lesivi del comune senso del pudore;
- diffondere prodotti informativi lesivi dell'onorabilità, individuale e collettiva;
- diffondere prodotti informativi di natura politica, se non espressamente autorizzati da fonti legislative o regolamentari;
- diffondere informazioni riservate di qualsiasi natura.

La navigazione in internet forma oggetto di controllo da parte degli amministratori di sistema, nel rispetto dei principi di pertinenza e non eccedenza secondo le modalità indicate nelle Linee Guida del Garante di cui alla Deliberazione n. 13 del 1 marzo 2007.

I sistemi software allo scopo predisposti saranno programmati e configurati in modo da cancellare periodicamente i dati relativi agli accessi Internet ed al traffico telematico secondo quanto previsto da tali Linee Guida del Garante.

Gli amministratori di sistema (centrale e periferici) cureranno, per ciascuna struttura, l'assegnazione degli indirizzi IP (Internet Protocol) all'interno della struttura provvedendo sempre a mantenere aggiornata, con uno storico di almeno due anni, la lista delle coppie "Indirizzo IP-Nome Utente" oppure "Indirizzo IP-MAC ADDRESS" assegnati. Non sarà quindi, a regime, consentito ed utilizzato alcun sistema di tipo DHCP per l'assegnazione dinamica dell'indirizzo IP di rete.

Non è consentito collegare alla rete di ARPACAL, anche tramite collegamento Wi-Fi, attrezzature di calcolo personali o comunque non di proprietà dell'Agenzia (desktop, notebook, palmari, smartphone) se non

preventivamente autorizzate dall'amministratore di sistema della struttura dove l'attrezzatura va collegata o direttamente dalla U.O. Sistemi Informativi Sicurezza e Privacy e fermo restando tutti i controlli automatici di blocco che saranno previsti. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente Regolamento.

Non è inoltre consentito collegare alla rete di ARPACAL apparati di rete (Access Point Wi-Fi, router, switch, etc.) se non preventivamente autorizzati dalla U.O. Sistemi Informativi Sicurezza e Privacy. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente Regolamento.

Uso della posta elettronica

La casella di posta elettronica assegnata da ARPACAL all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Attualmente ARPACAL utilizza caselle di posta elettronica non definite su propri server ma utilizzando un sistema in outsourcing. Le caselle hanno una capacità di memorizzazione della posta normalmente limitata a 100 MB, è quindi necessario periodicamente provvedere allo svuotamento della casella stessa per evitare un messaggio di "user over quota".

Le credenziali di accesso per l'uso di caselle mail sono rilasciate dall' apposito referente dell'Agenzia con il ruolo di amministratore di sistema delle caselle mail in outsourcing.

È fatto divieto di utilizzare le caselle di posta elettronica di ARPACAL (*del tipo nominativo@arpacal.it*) per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione. Il mancato rispetto di tale circostanza può generare comunque "spam" sui server del fornitore del servizio mail in outsourcing con rischio di intasamento delle caselle degli altri utilizzatori, disservizi e potenziale richiesta di maggiori oneri da parte del medesimo fornitore.

Non è consentito, inoltre, inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria.

È buona norma evitare l'uso della casella per l'invio/ricezione di messaggi completamente estranei al rapporto di lavoro. La casella di posta deve essere mantenuta in ordine, cancellando i documenti inutili/obsoleti e soprattutto allegati ingombranti.

Ogni comunicazione inviata/ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per ARPACAL deve essere visionata e/o autorizzata dal Dirigente Responsabile dell'incaricato, valendo comunque tutte le procedure in essere per la corrispondenza ordinaria.

Per la trasmissione di files all'interno di ARPACAL è possibile utilizzare la posta elettronica (prestando attenzione alla dimensione degli allegati) oppure prioritariamente, se possibile, le aree condivise sui server di ARPACAL per come opportunamente predisposte.

È vietato avviare e/o partecipare a catene telematiche (cosiddette "catene di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, non si deve in alcun caso accedere/attivare eventuali allegati a tali messaggi e si deve procedere immediatamente cestinando tale comunicazione.

La casella di posta di ogni singola struttura può essere utilizzata da più utenti secondo quanto stabilito dal Responsabile della struttura stessa.

In caso di assenza prolungata o improvvisa il singolo utente deve essere messo in condizioni di delegare un altro utente a leggere i propri messaggi e ad inoltrare quelli ritenuti importanti per lo svolgimento dell'attività lavorativa. A tal fine il responsabile del servizio mail server (attualmente tale persona responsabile, in capo alla Direzione Generale Settore Organizzazione, informerà gli utenti se il fornitore del servizio mail in outsourcing può consentire il rinvio automatico ad altre mail in caso di assenza prolungata, da intendersi come numero di giorni predefinito di assenza es. una settimana).

Gli utenti, previa autorizzazione ed in via eccezionale, possono utilizzare una propria casella di posta elettronica non istituzionale. In questo caso, se l'accesso avviene tramite postazioni di lavoro di proprietà di ARPACAL, la casella di posta può essere consultata solo in modalità webmail.

Le caselle personali non istituzionali non possono essere utilizzate per l'attività istituzionale. E' fatto divieto di inviare messaggi con contenuti che non rispettino la normativa sulla proprietà intellettuale.

Nel caso di costituzione di mailing list di tutto il personale di ARPACAL suddivise per categoria e per funzioni, l'iscrizione alle mailing list è automatica una volta assegnata la casella di posta istituzionale.

Le mailing list sono adibite alla diffusione d'informazioni di interesse generale e comunque di servizio rivolte al personale.

Hanno diritto ad utilizzare le mailing list del personale:

- il Direttore Generale, Scientifico ed Amministrativo;
- il Dirigente Responsabile del Personale;
- il Direttore di Dipartimento Provinciale.

Il Direttore Generale può estendere l'utilizzo alle organizzazioni sindacali ed alle RSU rappresentate nell'Agenzia e ad altri soggetti interni ad ARPACAL compresi gli altri membri degli organi di amministrazione che ne facciano espressa richiesta.

PARTE QUARTA

Controlli e responsabilità

L'uso dei dispositivi informatici della ARPACAL per l'effettuazione di trattamento di dati personali deve avvenire attenendosi alle disposizioni in materia di privacy e di misure minime di sicurezza indicate nella lettera d'incarico ai sensi del D.Lgs n. 196/2003 e s.m.i.

Monitoraggio

La U.O. Sistemi Informativi Sicurezza e Privacy, per il tramite degli amministratori di sistema, effettua monitoraggi periodici **su dati aggregati non riconducibili al singolo utente** allo scopo di verificare l'attuazione del presente regolamento, i possibili rischi legati alla sicurezza informatica e le possibili problematiche legate all'utilizzo delle **risorse informatiche e telematiche**.

Questi monitoraggi possono essere classificati in:

- analisi del traffico di rete: effettuati attraverso specifici **log** dei dispositivi di rete;
- analisi del traffico Internet: effettuati attraverso specifici **log** dei dispositivi di connessione ad Internet;
- inventari di **Hardware e Software** effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti ai cosiddetti domini di rete. Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali. I dati del traffico telematico verranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telematico.

L'Agenzia si riserva la facoltà di procedere alla rimozione di ogni **file** o **applicazione** che riterrà pericolosa per la sicurezza del sistema informatico ovvero acquisita o installata in violazione del presente Regolamento.

Anche l'attività degli amministratori di sistema sarà soggetta a controlli, secondo le indicazioni del Garante del 27 novembre 2008 pubblicato sulla Gazzetta Ufficiale n. 300 del 24 dicembre 2008.

Inoltre, l'elenco degli amministratori di sistema sarà riportato sul DPS, incluse le funzioni agli stessi assegnate per esigenze dei Titolari di trattamento.

Controlli

ARPACAL effettua controlli periodici per verificare il rispetto del presente Regolamento.

Nel caso in cui emergano eventi dannosi, situazioni di pericolo o utilizzi delle **risorse informatiche e telematiche** non rispettosi del presente Regolamento, la U.O. Sistemi Informativi Sicurezza e Privacy potrà adottare le misure più idonee a consentire la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti alla Direzione/Settore/Servizio o al Dipartimento Provinciale/Centro, o strutture ad essi equiparate, nel cui ambito sono state rilevate le anomalie di utilizzo.

Il controllo, **su dati aggregati non riconducibili al singolo utente**, si concluderà con una comunicazione al Direttore/Dirigente/ Centro o struttura equiparata che, dopo avere informato in forma generalizzata gli **utenti** delle irregolarità di utilizzo rilevate, li inviterà ad attenersi scrupolosamente alle disposizioni del presente Regolamento.

Qualora le anomalie e irregolarità dovessero persistere saranno effettuati controlli su base individuale.

In nessun caso verranno poste in essere azioni sistematiche volte ad un monitoraggio puntuale delle attività informatiche svolte da ogni utente:

- la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica);
- la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore;
- la memorizzazione di quanto visualizzato sul monitor.

I controlli di cui al comma precedente possono riguardare anche i software caricati sulle stazioni di lavoro adoperate dagli **utenti**, al fine di verificarne la regolarità con riguardo alle disposizioni vigenti in materia di proprietà intellettuale.

È fatta salva la possibilità di effettuare controlli ad hoc anche nelle ipotesi in cui vengano segnalati utilizzi di **risorse informatiche e telematiche** idonei a causare danni all'Amministrazione o a ledere i diritti di terzi.

Sanzioni

Qualora, ad esito dei controlli, la U.O. Sistemi Informativi Sicurezza e Privacy rilevi degli utilizzi anomali delle risorse informatiche e telematiche, provvederà tempestivamente ad informare il

dirigente della Struttura presso la quale l'**utente** presta la propria attività per gli opportuni e/o dovuti provvedimenti, eventualmente anche disciplinari, consequenziali.

PARTE QUINTA

Norme di chiusura

1. Con riferimento ai controlli di cui al presente Titolo, il presente regolamento costituisce fonte di preventiva e completa informazione nei confronti degli **utenti**.
2. Tale Regolamento è inviato alle OO.SS. ed alle RSU agenziali per l'opportuna conoscenza.
3. L'accesso alle risorse informatiche e telematiche di ARPACAL richiede l'integrale e incondizionata accettazione delle disposizioni del presente Regolamento.
4. Ad approvazione avvenuta tale Regolamento sarà inviato a tutti i dipendenti dell'ARPACAL.

Informativa agli utenti ai sensi dell'art. 13 D.Lgs. 196/2003

Il Direttore Generale di ARPACAL è il TITOLARE principale del trattamento dei dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori. Il Direttore Amministrativo ed il Direttore Scientifico sono gli ulteriori Titolari per gli ambiti di propria competenza.

FINALITA' del trattamento è la verifica del corretto utilizzo delle risorse informatiche, della posta elettronica e della rete Internet/Intranet nel rapporto di lavoro.

MODALITA' del trattamento: gli amministratori di sistema centrali e periferici o personale tecnico esterno autorizzato dal Direttore Generale e/o dal Dirigente U.O. Sistemi Informativi Sicurezza e Privacy effettueranno il trattamento dei dati con strumenti informatici.

COMUNICAZIONE DEI DATI: il trattamento di verifica è effettuato con gradualità e per aree aggregate per cui i dati non vengono comunicati con riferimento al trattamento del singolo lavoratore; la comunicazione, nel caso in cui si accerti un uso indebito della singola postazione, sarà data al Direttore della Struttura Operativa alla quale appartiene **l'utente** per la valutazione del caso sotto il profilo **disciplinare.**

DIRITTI DELL'INTERESSATO: Il dipendente potrà far valere i diritti di cui all'art. 7 del D.Lgs. 196/03 facendo pervenire richiesta scritta al Titolare principale del Trattamento dati che è il **Direttore Generale** o al Direttore apicale della struttura nella quale opera.

Aggiornamento e revisione

Tutti gli utenti possono sottoporre all'esame del U.O. Sistemi Informativi Sicurezza e Privacy di ARPACAL eventuali proposte scritte per l'integrazione e/o la rettifica del presente documento.

Il presente Regolamento è soggetto a revisione senza una frequenza minima e comunque su base di reale necessità o secondo l'evoluzione del Sistema Informatico di ARPACAL.

ALLEGATI

Appendice A: glossario tratto dal D.Lgs. n. 196/2003

a.**"trattamento",** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b.**"dato personale",** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c.**"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;

d.**"dati sensibili",** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e. **"dati giudiziari",** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f. **"titolare",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g. **"responsabile",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h. **"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i. **"interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

j. **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

k. **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

l. **"banca dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

m. **"Garante",** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675

n. **"comunicazione elettronica"**, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

o. **"reti di comunicazione elettronica"**, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

p. **"posta elettronica"**, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

q. **"misure minime",** il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

r. **"strumenti elettronici",** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

s. **"autenticazione informatica",** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

t. **"credenziali di autenticazione",** i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

u. **"parola chiave",** componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

v. **"profilo di autorizzazione",** l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

w. **"sistema di autorizzazione",** l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Modello di richiesta accesso ed uso risorse informatiche e telematiche di ARPACAL

- Al Direttore Generale/Scientifico/Amministrativo

(oppure)

- Al Direttore Dipartimento Provinciale di

(oppure)

- Al Direttore CFS/CE

- Alla U.O. Sistemi Informativi Sicurezza e Privacy

COGNOME UTENTE	
NOME UTENTE	
STRUTTURA DI APPARTENENZA	
PERSONAL COMPUTER **(PC)** ASSEGNATO (MARCA, MODELLO E SERIAL NUMBER)	
MONITOR PC ASSEGNATO (MARCA, MODELLO E SERIAL NUMBER)	
TIPO E VERSIONE SISTEMA OPERATIVO PC	
PRODUCT KEY SISTEMA OPERATIVO PC	
APPLICAZIONI INSTALLATE O DA UTILIZZARE SU PC	
NOTEBOOK **(NB)** ASSEGNATO (MARCA, MODELLO E SERIAL NUMBER)	
CARATTERISTICHE NB ASSEGNATO RAM, CAPACITA' DISCO, MAC ADDRESS SCHEDA DI RETE WIRELESS E MAC ADDRESS SCHEDA RJ45	
TIPO E VERSIONE SISTEMA OPERATIVO NB	
PRODUCT KEY SISTEMA OPERATIVO NB	

APPLICAZIONI INSTALLATE E DA UTILIZZARE SU NB	
CASELLA/E DI POSTA ASSEGNATA/E	
DELEGATO ALLA CASELLA DI POSTA IN CASO DI ASSENZA	
NECESSITA' DI ACCESSO AD AREE CONDIVISE SU SERVER (SI/NO). SE SI INDICARE LE NECESSITA'	
RICHIESTO ACCESSO INTRANET (SI/NO)	
RICHIESTO ACCESSO INTERNET (SI/NO)	
CON LA FIRMA A LATO DELLA PRESENTE DICHIARO DI AVER PRESO VISIONE E DI ACCETTARE IL REGOLAMENTO SULL'USO DELLE RISORSE INFORMATICHE E TELEMATICHE DI ARPACAL NONCHE' DI AVER PRESO VISIONE DELLA SPECIFICA INFORMATIVA	_____
FIRMA DEL DIRETTORE/DIRIGENTE PER APPROVAZIONE DELLA RICHIESTA	_____