Proposta	n. PDEL-2024-140 del 10/12/2024
Deliberazione del Direttore Generale	n. DEL-2024-135 del 11/12/2024
Oggetto	Servizio Sistemi Informativi e Innovazione Digitale. Approvazione della "Policy utenti dei sistemi informativi di Arpae".
Dirigente proponente	Servizio Sistemi Informativi E Innovazione Digitale - Cicognani Matteo
Responsabile del procedimento	Cicognani Matteo

Questo giorno *11/12/2024* il Direttore Generale, Dott. Bortone Giuseppe, delibera quanto segue.

VISTI:

- il D.Lgs. 7 marzo 2005, n. 82 “Codice dell’Amministrazione digitale”;
- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, “Regolamento generale sulla protezione dei dati”, conosciuto anche come GDPR;
- il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali” (nel seguito anche Codice) come modificato ed integrato dal D.Lgs. 10 marzo 2023, n. 24;

RICHIAMATI:

- il D.P.R. n. 62/2013 - “Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165” - come da ultimo modificato dal D.P.R. n. 81/2023, con particolare riferimento all’art. 11 bis “Utilizzo delle tecnologie informatiche”;
- il Codice di comportamento aziendale di Arpae - approvato con D.D.G. n. 109/2024 - il cui art. 11 contiene specifiche disposizioni in merito all’utilizzo delle tecnologie informatiche rinviando, per quanto non previsto nel Codice medesimo, agli specifici disciplinari adottati dall’Agenzia;

PREMESSO:

- che la tutela del patrimonio delle informazioni riveste importanza strategica per Arpae, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice;
- che il sistema informativo regionale di Arpae è costituito da un’infrastruttura tecnologica molto articolata e complessa, formata da sistemi di elaborazione dati di varia natura, basi dati, apparati di rete e di sicurezza, sistemi software anche complessi;

CONSIDERATO:

- che si rende necessario assicurare maggiore organicità e coordinamento all’attività del personale incaricato di gestire e amministrare i sistemi informatici e telematici dell’Agenzia;
- che risulta inoltre necessario adottare ogni misura, tecnica ed organizzativa, volta a prevenire il rischio di utilizzo improprio delle strumentazioni informatiche in dotazione agli utenti e delle banche dati dell’Agenzia, nel rispetto del diritto alla riservatezza e dei diritti dei lavoratori, nonché a promuovere l’utilizzo corretto degli strumenti messi a disposizione per lo svolgimento dell’attività ed a verificare l’utilizzo corretto dell’infrastruttura di rete;

CONSIDERATO altresì:

- che la gestione tecnica e la manutenzione degli impianti di elaborazione o di sue componenti comportano in molti casi attività che vanno considerate a tutti gli effetti alla stregua di trattamenti

di dati personali;

RICHIAMATA:

- la D.D.G. n. 41 del 26/04/2023 che individua nella figura del Direttore Generale dell'Agenzia il Titolare del trattamento dei dati personali (ovvero del soggetto a cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso quello della sicurezza), e nella figura dei Responsabili delle strutture i soggetti attuatori degli adempimenti previsti dalla normativa in materia di protezione dei dati personali;

RILEVATO:

- che il Servizio Sistemi informativi e Innovazione digitale ha predisposto il documento "Policy utenti dei sistemi informativi di Arpae", allegato sub A) al presente atto quale parte integrante e sostanziale, che descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo di Arpae al fine di:
  - ottimizzare l'impiego delle risorse dell'Agenzia;
  - introdurre regole di corretto utilizzo delle strumentazioni e credenziali informatiche nel contesto organizzativo dell'Agenzia;
  - prevenire il rischio di utilizzi impropri degli strumenti forniti;
  - ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito dei dati e delle informazioni;
  - garantire la disponibilità dei servizi e il rispetto delle norme sul diritto d'autore;
  - responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
  - definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze di un utilizzo indebito delle risorse tecnologiche;

SPECIFICATO:

- che per "sistema informativo" si intende il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate alla acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni;
- che per "utenti dei sistemi informativi di Arpae" si intendono tutti i soggetti che usufruiscono dei servizi del sistema informativo di Arpae il cui accesso è consentito tramite accreditamento al sistema di gestione delle identità denominato Active Directory e al sistema di gestione delle identità di Google Workspace (nel caso di richiesta di accesso a strumenti che prevedono questo tipo di autenticazione);

- che le risorse tecnologiche a disposizione degli utenti comprendono:
  - la dotazione hardware e software (incluso lo smartphone aziendale) della Postazione di lavoro personale assegnata agli utenti dell'agenzia;
  - gli strumenti standard di produttività personale e di workgroup;
  - le postazioni di lavoro condivise per specifici utilizzi e relative dotazioni hardware e software (a titolo esemplificativo non esaustivo le postazioni all'interno dei laboratori analitici, le postazioni dei front-office, le postazioni dedicate ai tirocinanti, le postazioni dedicate all'utilizzo di specifici software che richiedano software o hardware specifici e debbano essere utilizzati, presso i locali di Arpae, da più operatori);

DATO ATTO INOLTRE:

- che in data 8/08/2024 il Responsabile del Servizio Sistemi informativi e Innovazione digitale ha inviato al Comitato di Direzione il documento di cui trattasi ai fini dell'acquisizione di osservazioni e/o proposte di modifica sul testo;

RITENUTO:

- opportuno approvare la "Policy utenti dei sistemi informativi di Arpae", allegata sub A) al presente atto quale parte integrante e sostanziale;
- di disporre la più ampia diffusione della "Policy utenti dei sistemi informativi di Arpae" all'interno dell'Agenzia;

PRECISATO:

- che quanto previsto nella "Policy utenti dei sistemi informativi di Arpae" integra e specifica le disposizioni già contenute, in materia di utilizzo delle tecnologie informatiche, nel Codice di comportamento dei dipendenti pubblici (D.P.R. n. 62/2013 e D.P.R. n. 82/2023) e nel Codice di comportamento aziendale di Arpae (D.D.G. n. 109/2024);

SU PROPOSTA:

- del Responsabile del Servizio Sistemi Informativi e Innovazione Digitale di Arpae, Dott. Matteo Cicognani, il quale ha espresso parere favorevole in merito alla regolarità amministrativa del presente atto;

ACQUISITI:

- il parere favorevole del Direttore Amministrativo, Dott.ssa Lia Manaresi, e del Direttore Tecnico, Dott. Eriberto de' Munari, ai sensi dell'art. 9 della L.R. n. 44/1995;

DATO ATTO:

- che il responsabile del procedimento è lo stesso Dott. Matteo Cicognani, Responsabile del

Servizio Sistemi Informativi e Innovazione Digitale;

DELIBERA

1. di approvare la “Policy utenti dei sistemi informativi di Arpae Emilia-Romagna”, allegata sub A) al presente atto quale parte integrante e sostanziale, finalizzata a definire le regole tecniche ed organizzative da applicare per l’utilizzo di strumentazioni informatiche da parte degli utenti che accedono al sistema informativo di Arpae Emilia-Romagna;
2. di applicare la suddetta Policy a tutti i soggetti che usufruiscono dei servizi del sistema informativo di Arpae il cui accesso è consentito tramite accreditamento al sistema di gestione delle identità denominato Active Directory e al sistema di gestione delle identità di Google Workspace (nel caso di richiesta di accesso a strumenti che prevedono questo tipo di autenticazione);
3. di precisare che quanto previsto nella “Policy utenti dei sistemi informativi di Arpae” integra e specifica le disposizioni già contenute, in materia di utilizzo delle tecnologie informatiche, nel Codice di comportamento dei dipendenti pubblici (D.P.R. n. 62/2013 e D.P.R. n. 82/2023) e nel Codice di comportamento aziendale di Arpae (D.D.G. n. 109/2024);
4. di disporre la più ampia diffusione della “Policy utenti dei sistemi informativi di Arpae” all’interno dell’Agenzia.

PARERE: FAVOREVOLE
IL DIRETTORE AMMINISTRATIVO
Firmato digitalmente
Dott.ssa Manaresi Lia

PARERE: FAVOREVOLE
IL DIRETTORE TECNICO
Firmato digitalmente
Dott. de’ Munari Eriberto

IL DIRETTORE GENERALE
Firmato digitalmente
Dott. Bortone Giuseppe

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire [1], come file separati dal testo del provvedimento sopra riportato:

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

arpae
agenzia
prevenzione
ambiente energia
emilia-romagna

POLICY UTENTI

DEI SISTEMI INFORMATIVI DI ARPAE

Indi

PREMESSA....4
1 SCOPO ED OBIETTIVI.... 4
2 CAMPO DI APPLICAZIONE....4
3 LE DOTAZIONI INFORMATICHE PERSONALI (PdL)....5
3.1 LE POSTAZIONI DI LAVORO....5
3.2 LA DOTAZIONE SOFTWARE DELLA POSTAZIONE DI LAVORO.... 6
3.2.1 Postazioni di Lavoro condivise....6
3.4 I SERVIZI DI STAMPA, FOTOCOPIA, SCANNER.... 6
3.4 CORRETTO UTILIZZO E CONSERVAZIONE DELLE DOTAZIONI DI LAVORO....7
3.5 INTERVENTI SULLE POSTAZIONI DI LAVORO DA PARTE DEL SERVIZIO DI ASSISTENZA UTENTI....7
4 LE CREDENZIALI DI IDENTIFICAZIONE INFORMATICA E L'ATTIVAZIONE DEI SERVIZI.... 7
4.1 COSA SONO LE CREDENZIALI DI IDENTIFICAZIONE INFORMATICA....8
4.2 ASSEGNAZIONE DELLE CREDENZIALI AL PERSONALE.... 8
4.3 ASSEGNAZIONE DELLE CREDENZIALI A SOGGETTI ESTERNI....9
4.3.1 Procedura di primo accreditamento dei soggetti esterni.... 9
4.3.3 Procedure di proroga, cessazione anticipata e cessazione ordinaria dell'accreditamento....9
4.3.4 Conservazione dei documenti relativi alle richieste e variazioni dell'accreditamento.... 9
4.4 Sospensione e Cancellazione delle credenziali....10
4.5 GESTIONE DELLE CREDENZIALI.... 10
4.5.1 PROTEZIONE DELLE CREDENZIALI E AZIONI IN CASO DI FURTO.... 10
4.5.2 IMPOSTAZIONE DELLE PASSWORD.... 11
4.6 ATTIVAZIONE E REVOCA DI APPLICAZIONI E SERVIZI DEL SISTEMA INFORMATIVO/INFORMATICO ARPAE. 11
5 UTILIZZO DI POSTAZIONI DI LAVORO PERSONALI.... 11
5.1 PREVENZIONE E SALVAGUARDIA DEI DATI....12
5.2 PREVENZIONE E SALVAGUARDIA DELLE POSTAZIONI DI LAVORO PORTATILI....12
5.3 UTILIZZO DI SMARTPHONE E TABLET FORNITI DALL' AGENZIA....12
5.5 UTILIZZO DEI DISPOSITIVI NON FORNITI DALL'AGENZIA.... 14
5.6 UTILIZZO DI SMARTPHONE E TABLET PERSONALI PER L'ACCESSO A DATI E SERVIZI DELL'AGENZIA.... 14
6 UTILIZZI DELLA RETE ARPAE.... 15
7 POSTA ELETTRONICA.... 15
7.1 UTILIZZO DELLA POSTA ELETTRONICA.... 15
7.3 SUGGERIMENTI PER LA PREVENZIONE DA MALWARE.... 16
8 FIRMA ELETTRONICA.... 17
9 NAVIGAZIONE IN INTERNET.... 17
10 PROTEZIONE ANTIVIRUS....17
11 GESTIONE DEI LOG....18
12 PREVENZIONE E GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA....18
13 PROTEZIONE DEI DATI TRATTATI SENZA L'UTILIZZO DI STRUMENTI ELETTRONICI.... 18
14 RECUPERO DEI DATI DA PARTE DELL'ENTE IN ASSENZA DELL'UTENTE E INDICAZIONE DEL FIDUCIARIO.. 19
14.1 RECUPERO DATI IN CASO DI ASSENZE PROGRAMMATE.... 20
14.2 RECUPERO DATI IN CASO DI ASSENZE NON PROGRAMMATE CON INDICAZIONE DEL FIDUCIARIO..... 20

14.3 RECUPERO DATI IN CASO DI ASSENZE CON MANCATA INDICAZIONE DEL FIDUCIARIO..... 21
14.4 AUTORIZZAZIONE ALL'UTILIZZO DELLA CASELLA DI POSTA ELETTRONICA AD ALTRI COLLABORATORI. 21
15 Sicurezza e PROTEZIONE DEI DATI..... 22
16 RUOLI E RESPONSABILITÀ..... 23
17 GLOSSARIO..... 24

PREMESSA

L'Agenzia Regionale per la prevenzione l'Ambiente e l'Energia della Regione Emilia-Romagna, (di seguito denominata "Agenzia" o "Arpae"), nell'esercizio dell'attività istituzionale opera prestando attenzione alla sicurezza delle informazioni perseguendo elevati livelli di sicurezza del proprio sistema informativo.
A tal fine Arpae si impegna ad adottare ogni misura, tecnica ed organizzativa, volta a prevenire il rischio di utilizzo improprio delle strumentazioni informatiche in dotazione e delle banche dati dell'Agenzia, nel rispetto del diritto alla riservatezza e dei diritti dei lavoratori e a promuovere, attraverso l'emanazione della presente policy, l'utilizzo corretto degli strumenti messi a disposizione per lo svolgimento dell'attività lavorativa.

1 SCOPO ED OBIETTIVI

La presente policy descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo di Arpae.

Ai fini della presente policy, si intende per "sistema informativo" il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate alla acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.

Le risorse tecnologiche dell'Agenzia a disposizione degli utenti comprendono:

- la dotazione hardware e software (incluso lo smartphone aziendale) della Postazione di lavoro personale assegnata agli utenti dell'agenzia;
- gli strumenti standard di produttività personale e di workgroup;
- le postazioni di lavoro condivise per specifici utilizzi e relative dotazioni hardware e software (a titolo esemplificativo non esaustivo le postazioni all'interno dei laboratori analitici, le postazioni dei front-office, le postazioni dedicate ai tirocinanti, le postazioni dedicate all'utilizzo di specifici software che richiedano software o hardware specifici e debbano essere utilizzati, presso i locali di Arpae, da più operatori).

Le disposizioni qui contenute hanno la finalità di:

- ottimizzare l'impiego delle risorse dell'Agenzia;
- introdurre regole di corretto utilizzo delle strumentazioni e credenziali informatiche nel contesto organizzativo dell'Agenzia;
- prevenire il rischio di utilizzi impropri degli strumenti forniti;
- ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito dei dati e delle informazioni;
- garantire la disponibilità dei servizi e il rispetto delle norme sul diritto d'autore;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze di un utilizzo indebito delle risorse tecnologiche.

Tutta la modulistica relativa all'applicazione del presente policy è reperibile sul sito Intranet dell'Agenzia.

Nelle more del completamento della pubblicazione di tutta la modulistica dedicata su Aggiornati è possibile inviare le richieste relative all'applicazione della presente policy mediante lo strumento di supporto informatico dell'ente.

Quanto riportato nella presente policy non esaurisce tutte le prescrizioni contenute nelle vigenti normative relativamente ad illeciti disciplinari, civili e penali, con particolare riferimento alle violazioni di

sicurezza e ai reati informatici.

2 CAMPO DI APPLICAZIONE

La presente policy si applica a tutti i soggetti che accedono ai servizi del sistema informativo di Arpae il cui accesso è consentito tramite accreditamento al sistema di gestione delle identità denominato Active Directory e al sistema di gestione delle identità di Google Workspace (nel caso di richiesta di accesso a strumenti che prevedono questo tipo di autenticazione).

Nel seguito della policy, i soggetti di cui sopra sono denominati "utenti".

3 LE DOTAZIONI INFORMATICHE PERSONALI

In relazione alla tipologia di rapporto di lavoro/collaborazione instaurato e alle mansioni assegnate dall'Amministrazione, il SIID assegna agli utenti una postazione di lavoro per l'accesso alla rete e ai servizi del sistema informativo di Arpae, un insieme di dotazioni software individuali e servizi di stampa, fotocopie e scanner con configurazione predisposta per assicurare la tutela della privacy e la riservatezza dei dati e delle informazioni trattate.

La postazione di lavoro (nel seguito PDL) può essere PERSONALE (se assegnata al singolo utilizzatore ad uso esclusivo) o CONDIVISA (se destinata ad un gruppo omogeneo di utenti per esigenze particolari).

Poiché le due tipologie hanno finalità diverse, anche la loro configurazione si differenzia: in generale la postazione personale è dotata di un pc portatile con configurazione standard, quella condivisa è dotata di un pc fisso con installati software dedicati ad attività specifiche.

Per utenti esterni (ad esempio: consulenti o collaboratori a titolo gratuito) che abbiano necessità di accedere ai servizi del sistema informativo ARPAE l'eventuale assegnazione di strumentazione idonea viene valutata congiuntamente dal SIID e dal dirigente Responsabile del Servizio di riferimento del collaboratore il quale, in caso di esito positivo dell'istruttoria, diviene responsabile per la consegna e per il recupero di tale dotazione al termine del rapporto di collaborazione.

In conformità a quanto previsto nei vigenti Codici di comportamento e disciplinari ogni utente è responsabile del corretto impiego delle risorse messe a sua disposizione dall'Agenzia.

Le postazioni informatiche assegnate devono essere utilizzate unicamente per lo svolgimento dell'attività lavorativa.

3.1 LE POSTAZIONI DI LAVORO

La tipologia e le caratteristiche delle postazioni di lavoro sono definite dal SIID, tenuto conto delle esigenze di lavoro rilevate per gruppi di utenti omogenei, dell'evoluzione tecnologica e del rapporto tra qualità, costi ed efficienza delle tecnologie disponibili a mercato.

Le postazioni di lavoro hanno caratteristiche minime comuni costituite da:

- un sistema operativo omogeneo e sicuro (dal punto di vista della possibilità di ricevere aggiornamenti di sicurezza rilasciati dal fornitore);
- una dotazione di applicativi individuali di base omogenei e standardizzati;
- un insieme di tecnologie che abilitano all'accesso alla rete ARPAE e a tutti i servizi applicativi dell'Agenzia, compresi eventuali certificati e/o dispositivi per il controllo delle identità del

dispositivo e dell'utente;
- la possibilità di accesso da parte di amministratori di sistema per l'erogazione dei servizi di assistenza remota e aggiornamento automatico;
- una configurazione omogenea che possa garantire la sicurezza della postazione stessa.

La postazione di lavoro personale per tutti i dipendenti Arpae, a prescindere dall'uso in ufficio, o in lavoro agile, è costituita da:

- uno smartphone,
- una SIM ricaricabile fonia e dati associata a un numero aziendale;
- un PC notebook con accessori (zaino, cuffie, mouse).

Le postazioni di lavoro sono protette, in caso di assenza, anche temporanea, tramite la sospensione o il blocco della sessione di lavoro. A tale fine è impostata automaticamente l'attivazione dello screen saver in un periodo di tempo congruo e definito dal SIID al fine di impedire la lettura o la modifica dei dati presenti a video.

Allo scopo di proteggere dati personali, sensibili e/o giudiziari e la sicurezza delle postazioni di lavoro, è vietato collegare supporti rimovibili o altre tipologie di dispositivi di proprietà dell'utente alle postazioni di lavoro dell'Agenzia.

3.2 LA DOTAZIONE SOFTWARE DELLA POSTAZIONE DI LAVORO

Ogni postazione di lavoro (PdL) è dotata di una configurazione base costituita dai seguenti software applicativi individuali:

- un sistema antimalware e EDR (Endpoint Detection and Response);
- un sistema di protezione della navigazione su web che monitora e registra in tempo reale il traffico e applica le regole di sicurezza dell'Agenzia;
- un browser configurato centralmente per l'accesso a tutti i servizi applicativi dell'Agenzia;
- un client VPN per garantire l'accesso alla rete interna dell'Agenzia quando si utilizza una rete pubblica o una rete diversa da quella di Arpae.

A tutti i lavoratori di Arpae sarà inoltre fornito l'accesso al sistema di produttività e collaboration in Cloud scelto dall'Agenzia, e in modo particolare la possibilità di utilizzare:

- un pacchetto di strumenti di produttività individuale;
- una casella di posta elettronica individuale;
- uno spazio di archiviazione individuale;
- uno spazio di archiviazione condivisa.

Per i collaboratori esterni l'accesso a tali servizi Cloud è previsto solo per ragioni di sicurezza o di opportunità qualora sia stato definito nei contratti di fornitura o qualora si dimostri l'impossibilità di operare e/o collaborare con ARPAE con strumenti alternativi di proprietà dei collaboratori esterni e/o dei loro datori di lavoro.

La postazione di lavoro è configurata e gestita dal SIID nel rispetto del principio di standardizzazione di tutte le postazioni di lavoro dell'Agenzia.

Esiste un catalogo centralizzato di software installabile sulle postazioni di lavoro definito e mantenuto dal SIID; gli utenti possono richiedere l'installazione di un software compreso nella lista o possono proporre l'inserimento di un nuovo software nella lista qualora sia di interesse comune a un gruppo omogeneo di utenti e rispetti i requisiti di sicurezza, economicità e idoneità funzionale.

Qualora la richiesta riguardi dotazioni software coperte da licenze onerose, la richiesta di installazione deve essere formulata dal responsabile della struttura.

3.3 Postazioni di Lavoro condivise

All'interno dei locali delle sedi Arpae possono essere installate e mantenute postazioni di lavoro condivise generalmente realizzate con pc desktop.

Tali postazioni sono assegnate al Dirigente Responsabile della struttura che ne fa richiesta e non sostituiscono le postazioni di lavoro personali degli utenti.

Tali postazioni possono essere mantenute, in particolare, per:

- l'utilizzo di strumentazione che necessiti di una connettività basata su schede hw specifiche, e/o versioni specifiche di sw con licenze non attribuibili agli utenti, e/o sistemi di sicurezza basati su "chiavi hardware";
- utilizzo in uffici in cui il personale può avvicendarsi anche più volte nel corso della giornata;
- utilizzo da parte di utenti esterni che debbano lavorare presso le sedi Arpae;
- postazioni di controllo informatico per apparati della sede (dedicate a uso esclusivo del personale SIID).

3.4 I SERVIZI DI STAMPA, FOTOCOPIA, SCANNER

Arpae è dotata, per i servizi di stampa, di apparati multifunzioni acquisiti a noleggio. Questi dispositivi sono in grado di offrire servizi di stampa, fotocopia e scanner attraverso un unico hardware.

Tutti gli utenti dell'Agenzia possono accedere a tutte le stampanti/copiatrici multifunzione, indipendentemente dalla loro collocazione fisica, e sono configurate dall'assistenza su richiesta.

Tutti gli utenti hanno la possibilità di eseguire scansioni e di archiviare i file digitalizzati su cartelle di rete o di inviarli ad una casella di posta elettronica dell'Agenzia tramite email.

Le stampanti personali e le stampanti diverse dalle stampanti multifunzione, ad eccezione di quelle utilizzate per la stampa delle etichette, in uso presso le strutture dell'Agenzia non sono coperte dai contratti di manutenzione gestiti dal SIID che non garantisce più l'approvvigionamento dei materiali consumabili connessi.

In un'ottica di dematerializzazione degli archivi e dei flussi documentali, in linea con le recenti disposizioni normative (cfr. art. 47, comma 2, lett. c, D. Lgs. n. 82/2005 - Codice dell'Amministrazione Digitale - CAD) ed in materia di protezione dei dati, ARPAE ha disposto la dismissione del FAX, al fine di privilegiare esclusivamente le comunicazioni di tipo telematico e la ricezione di documenti informatici tra pubbliche amministrazioni e da parte della cittadinanza.

3.5 CORRETTO UTILIZZO E CONSERVAZIONE DELLE DOTAZIONI DI LAVORO

Le dotazioni informatiche di lavoro, insieme agli accessori fisici e alle dotazioni software individuali, devono essere:

- consegnate ad ogni nuovo utente con la configurazione standard di base;
- utilizzate e conservate con diligenza dall'utente al fine di ottimizzare l'impiego delle risorse dell'Agenzia, il risparmio energetico e l'impatto ambientale, nel rispetto della presente policy, del codice di comportamento aziendale di Arpae e dei piani aziendali di azione per il risparmio e l'efficienza energetica;
- utilizzate in modo pertinente alle specifiche finalità della propria attività e di quelle della propria

organizzazione;
- custodite dall'utente anche in caso di trasferimento di sede e struttura dell'utente medesimo insieme a tutte le altre dotazioni strumentali personali;
- restituite dall'utente in caso di cessazione del rapporto di lavoro o del rapporto di collaborazione con Arpae e comunque non oltre l'ultimo giorno previsto dai documenti che ufficialmente disciplinano tale rapporto di lavoro: il dirigente della struttura a cui il collaboratore è assegnato deve presidiare affinché la restituzione sia effettuata nei termini previsti e nel caso questo non avvenga dovrà provvedere a contattare il collaboratore per il recupero della dotazione;
- prive di dati conservati sul disco rigido del sistema: le postazioni di lavoro non sono di norma sottoposte ad attività di backup. Gli eventuali dati e documenti devono essere memorizzati sui file server aziendali, negli spazi di archiviazione in cloud ufficiali dell'Agenzia, all'interno degli applicativi aziendali o su dispositivi di archiviazione esterni forniti dall'ente. In caso di furto o smarrimento o rottura del pc, Arpae non garantisce il recupero delle informazioni in esso contenute.

Le dotazioni restituite, ritirate per riparazione o sostituite per aggiornamento della dotazione, vengono configurate prima della nuova assegnazione in modo da cancellare ogni dato preesistente e riportate alla configurazione standard del momento.

3.6 INTERVENTI SULLE POSTAZIONI DI LAVORO DA PARTE DEL SERVIZIO DI ASSISTENZA UTENTI

In caso di appalto esterno per la gestione dell'assistenza informatica i dipendenti della ditta formalmente contrattualizzata e gli amministratori di sistema del SIID, possono collegarsi, in modalità remota, alla postazione di lavoro, allo scopo di assicurare l'assistenza tecnica, la sicurezza e l'operatività, effettuando operazioni di manutenzione e aggiornamento del software installato. Gli interventi sono effettuati dall'Assistenza esterna e dagli amministratori del SIID accedendo alla postazione con proprie credenziali e privilegi di amministratore di sistema.

Le modalità per l'attivazione dell'assistenza alle PDL sono riportate all'interno del portale Intranet Aziendale.

3.7 LA TELEFONIA FISSA

Le sedi di lavoro di Arpae sono dotate di apparati di telefonia fissa messi a disposizione dall'Agenzia per lo svolgimento dell'attività lavorativa, al pari delle dotazioni informatiche, assegnate a specifici utenti o a specifiche funzioni identificate dai dirigenti Responsabili di struttura su ciascuna sede e comunque in numero non superiore al 40% del numero dei dipendenti fisicamente assegnati alla sede.

I collaboratori di Arpae a cui sono dati in uso gli apparati di telefonia fissa, sono tenuti a utilizzarli in modo pertinente alle specifiche finalità dei propri compiti, nel rispetto delle esigenze di funzionalità generali e nell'ottica del contenimento dei costi.

A tal fine devono essere osservate alcune regole generali :

- utilizzare gli strumenti di telefonia fissa per lo svolgimento dell'attività lavorativa e in particolare limitare il ricorso alle chiamate personali (esclusivamente nei casi di effettiva e improrogabile necessità) e effettuare chiamate all'estero esclusivamente per esigenze di lavoro;
- proteggere i telefoni fissi, in caso di assenza, anche temporanea;
- non connettere alla rete apparati telefonici diversi da quelli ufficialmente assegnati dal SIID.

4 LE CREDENZIALI DI IDENTIFICAZIONE INFORMATICA E L'ATTIVAZIONE DEI SERVIZI

In adempimento alle misure di sicurezza previste dalla normativa vigente, si delineano di seguito le procedure e le regole d'uso per la gestione e assegnazione delle credenziali di identificazione informatica e le procedure per l'attivazione dei servizi assegnati all'utente.

L'accesso alle strumentazioni informatiche utilizzate per i trattamenti di dati personali è consentito nel rispetto delle disposizioni stabilite dal Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, dal D.Lgs. 30 giugno 2003, n. 196 e dalle deliberazioni di Arpae relative all'individuazione del titolare e dei soggetti attuatori della normativa in materia di protezione dei dati personali.

Il lavoratore che accede con la propria utenza ai sistemi informatici di Arpae è autorizzato al trattamento dei dati a cui accede con l'obbligo di osservare le disposizioni in materia di tutela e trattamento dei dati personali, secondo quanto previsto nei vigenti codici di comportamento e nella normativa di riferimento.

4.1 COSA SONO LE CREDENZIALI DI IDENTIFICAZIONE INFORMATICA

L'accesso al sistema informativo dell'Agenzia avviene attraverso autenticazione mediante credenziali di dominio Arpae o, limitatamente ai servizi che lo prevedono, mediante le credenziali Google Workspace.

Le credenziali di identificazione informatica consistono in un codice per l'identificazione dell'utente associato a una parola chiave riservata, conosciuta solamente dal medesimo (che può essere associato a un codice identificativo o a una parola chiave), oppure in una caratteristica biometrica dell'utente (anche questa può essere associata a un codice identificativo o a una parola chiave). Di seguito qualche esempio:

- credenziali di identificazione informatica basate su parola chiave segreta: le credenziali userid e password utilizzate per l'accesso alle risorse di dominio (postazioni di lavoro, server intranet, ecc.) o per l'accesso alle applicazioni con autenticazione non integrata;
- credenziali di identificazione informatica basate su caratteristica biometrica dell'utente: le credenziali (userid+impronta+pin) utilizzate per gli accessi ai dispositivi mobili tramite riconoscimento dell'impronta digitale.

4.2 ASSEGNAZIONE DELLE CREDENZIALI AL PERSONALE

Il rilascio delle credenziali di identificazione informatica agli utenti del sistema informativo è di competenza del SIID e può avvenire solo a seguito di richiesta e di trasmissione della determina dirigenziale da cui risulti evincibile l' instaurazione del rapporto di lavoro/collaborazione (a qualsiasi titolo) con Arpae

Per il personale acquisito con rapporto di lavoro subordinato (anche in posizione di comando) e per il personale con contratto di somministrazione di lavoro a tempo determinato, la richiesta e la trasmissione della determina è effettuata dal Servizio Risorse Umane

La richiesta di attivazione delle credenziali deve essere completa delle generalità dell'utente (Nome, Cognome, Codice Fiscale), della data di attivazione, della data di dismissione e, possibilmente, dell' elenco degli strumenti informatici per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle

abilitazioni di accesso ai sistemi informativi dovrà pervenire al SIID con richiesta formale.

Un utente può essere dotato di tre tipologie di account aziendali:

- l'account Active Directory (ArpaeID o credenziali di dominio) che sono costituite da uno "userid" (di norma composto dalla prima lettera del nome unitamente al cognome per esteso, esempio Mario Rossi -> mrossi) e da una password temporanea che dovrà essere modificata obbligatoriamente al primo accesso ai sistemi. Le credenziali di dominio permettono agli utenti di accedere ai personal computer e ad alcuni applicativi dell'Agenzia:
- l'account Google Workspace costituito da un indirizzo email (di norma composto dalla prima lettera del nome unitamente al cognome per esteso e dal dominio @arpae.it, esempio Mario Rossi -> mrossi@arpae.it) e da una password temporanea (che dovrà essere modificata obbligatoriamente al primo accesso) e da un sistema a due fattori che ne rafforza la sicurezza informatica;
  Le credenziali Google Workspace permettono di accedere alla casella di posta elettronica cloud, al pacchetto di strumenti di produzione individuale cloud e allo spazio di archiviazione cloud (personale o condiviso) e alla VPN Arpae;
- l'account relativo ad uno specifico applicativo. L'accesso agli applicativi viene configurato e rilasciato stabilendo, preventivamente, i ruoli strettamente necessari alle funzioni per cui gli utenti sono incaricati (compatibilmente al livello di responsabilità e al contesto in cui operano); l'autorizzazione concessa deve rispettare il principio di pertinenza, l'istanza dovrà pertanto essere opportunamente misurata dal soggetto richiedente.

4.3 ASSEGNAZIONE DELLE CREDENZIALI A SOGGETTI ESTERNI

Qualsiasi soggetto esterno ad Arpae che debba accedere presso le sedi dell'Agenzia o da remoto al sistema informativo, indipendentemente dalla tipologia del rapporto di lavoro/collaborazione, deve essere accreditato tramite il rilascio di una credenziale informatica.

Nel caso di collaboratori esterni (es. tirocinanti), la richiesta per il rilascio delle credenziali e la trasmissione della determinazione è a cura del Responsabile della struttura, o suo delegato, con il quale l'utente esterno si coordina nell'espletamento del proprio incarico: ad es. la determinazione di approvazione del tirocinio deve essere trasmessa al SIID dal Responsabile della struttura a cui il tirocinante è assegnato.

Ai possessori delle credenziali di identificazione informatica si applicano le medesime discipline in materia di Sistemi Informativi e privacy che si applicano ai dipendenti dell'Agenzia.

4.3.1 Procedura di primo accreditamento dei soggetti esterni

L'accreditamento avviene su istanza di un responsabile di struttura.

L'istanza di accreditamento, da far pervenire al SIID, dovrà riportare per ogni soggetto da accreditare i seguenti dati:

- Nome e Cognome;
- Luogo e data di nascita;
- Codice fiscale;
- Email personale;
- Azienda per cui opera il soggetto accreditato (se esiste);
- Inizio del periodo di accreditamento;
- Termine del periodo di accreditamento;
- Riferimento di protocollo all'atto che motiva l'accreditamento (Contratto di fornitura di servizi, Contratto di consulenza, Convenzione con soggetto esterno, tirocinio formativo, lavoro estivo

guidato, contratto gratuito, ecc.).

La durata dell'accreditamento non deve superare i termini del rapporto contrattuale del soggetto esterno.

4.3.2 Procedure di proroga, cessazione anticipata e cessazione ordinaria dell'accreditamento

In caso di proroga dell'accreditamento oltre i termini di scadenza, il Responsabile di struttura che ha avanzato l'istanza di accreditamento dovrà, entro 5 giorni lavorativi antecedenti la scadenza, avanzare richiesta di proroga con le medesime modalità utilizzate in sede di primo accreditamento.

Qualora il soggetto cessi l'attività prima della scadenza prevista, il Responsabile della struttura di assegnazione dovrà avanzare istanza di revoca con le medesime modalità utilizzate in sede di primo accreditamento.

La proroga dell'accreditamento è possibile solo se conseguente alla proroga del rapporto di collaborazione in essere al momento della precedente istanza di accreditamento.

4.3.3 Conservazione dei documenti relativi alle richieste e variazioni dell'accreditamento

I documenti relativi all'istanza di accreditamento potranno essere gestiti in formato elettronico all'interno del sistema di protocollo informatico/gestione documentale e saranno soggetti alle misure ivi già stabilite per la protezione dei dati personali.

4.4 Sospensione e Cancellazione delle credenziali

Al termine del rapporto di lavoro/collaborazione con Arpae, qualora non si sia proceduto con una istanza di proroga , le credenziali di accesso rilasciate all'utente vengono disattivate e non potranno più essere utilizzate per accedere ai sistemi informativi e alla posta elettronica aziendale. Se un'email viene spedita ad un account di posta sospeso il mittente riceve una risposta automatica che lo avverte della sospensione (fino alla effettiva eliminazione dell'account di posta).

Gli account disattivati sono definitivamente cancellati e con essi i dati collegati a tali account secondo i tempi indicati in apposita procedura relativa alla Gestione delle Identità digitali in Arpae.

Nelle more dell'emanazione della procedura relativa alla Gestione delle Identità digitali in Arpae, il tempo di conservazione degli account e dei dati ad essi correlati, inclusi i messaggi di posta elettronica e i file contenuti nel proprio drive personale, è fissato in 30 giorni; superato tale termine tutti i dati saranno cancellati.

Nessun utente di Arpae può fare richiesta di dati contenuti all'interno del sistema informativo collegati ad un account sospeso o cancellato al termine del rapporto di lavoro/collaborazione con Arpae.

Per garantire all'organizzazione di Arpae la possibilità di accedere a dati e documenti di lavoro ospitati negli spazi di archiviazione personali in cloud (principalmente il proprio Google Drive personale" identificato anche come "Il mio Drive") è necessario che l'utente possessore dei dati provveda a spostarli all'interno di cartelle di rete o all'interno di Google Drive Condivisi, già visibili ad altri colleghi, prima del termine del proprio rapporto di lavoro/collaborazione con Arpae.

4.5 GESTIONE DELLE CREDENZIALI

Ogni credenziale di identificazione informatica si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti.

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Le credenziali di identificazione informatica alle risorse di dominio e alle applicazioni sono immediatamente disattivate nel caso in cui un soggetto interrompa il suo rapporto di lavoro/ la sua collaborazione con l'Agenzia.

Le credenziali di identificazione informatica che non sono utilizzate da almeno sei mesi vengono disattivate, salvo quelle utilizzate per la gestione tecnica dagli amministratori dei sistemi informatici e quelle utilizzate per l'accesso ai sistemi e alle basi di dati dalle applicazioni.

4.5.1 PROTEZIONE DELLE CREDENZIALI E AZIONI IN CASO DI FURTO

Ciascun utente è responsabile della sicurezza delle proprie password e deve adottare le necessarie cautele per mantenerle segrete. Le password sono strettamente personali e non devono in nessun caso essere comunicate ad altri.

In caso di furto o sospetto furto delle credenziali l'utente è tenuto a seguire le procedure di seguito specificate:

- in caso di furto della componente riservata (password o PIN) è necessario, al primo accesso seguente al furto, cambiare la propria password o il proprio PIN e contattare immediatamente il SIID preposto alle problematiche di sicurezza informatica;
- in caso di furto o smarrimento del proprio token è necessario richiedere la sospensione immediata del certificato digitale al Certificatore. Si dovrà, poi, sporgere denuncia alle Autorità competenti e trasmettere al SIID la richiesta di revoca del certificato digitale allegando copia della denuncia di furto o smarrimento e darne comunicazione al DPO di Arpae.

4.5.2 IMPOSTAZIONE DELLE PASSWORD

Ciascun utente quando effettua l'accesso ad un sistema per la prima volta è tenuto a modificare e personalizzare la password di accesso che deve essere lunga almeno 8 caratteri per le credenziali di dominio e 10 caratteri per le credenziali Google.

Consigli per la corretta impostazione della password

Si raccomanda di:

- non impostare la password in modo che sia facilmente collegabile alla propria vita privata (per es. il nome o il cognome di familiari, la targa dell'auto, la data di nascita, la città di residenza, ecc.);
- non impostare come password parole comuni riportate in un vocabolario (esistono infatti programmi fraudolenti, utilizzati per la forzatura di password che si basano su ricerche sistematiche effettuate sulle parole comuni);
- scegliere password che contengono combinazioni di lettere maiuscole e minuscole, numeri, caratteri speciali (verifica caso per caso le indicazioni di sicurezza della password);
- non utilizzare la medesima password su sistemi differenti (per es. scegliere una password di dominio differente da quella di Google Workspace o dagli altri applicativi dell'Agenzia).

4.6 ATTIVAZIONE E REVOCA DI APPLICAZIONI E SERVIZI DEL SISTEMA INFORMATIVO/INFORMATICO ARPAE

La richiesta di attivazione e revoca dei servizi del sistema informativo di Arpae e l'installazione e la rimozione dei pacchetti software onerosi deve essere presentata dal Responsabile della struttura a cui l'utente è assegnato.

Ogni richiesta di attivazione e/o abilitazione ai servizi informatici dovrà riportare obbligatoriamente i riferimenti del soggetto accreditato a cui si intende assegnare la risorsa.

La procedura di attivazione e assegnazione di un servizio del sistema informativo/informatico Arpae ad un utente accreditato sul dominio risponde ai seguenti requisiti:

1. Il responsabile della struttura assegnataria avanza richiesta in forma scritta e tracciabile al SIID, anche in forma dematerializzata, di assegnare un servizio o un pacchetto software oneroso all'utente accreditato;
2. Il SIID valuta la richiesta in base ai criteri di sicurezza informatica, interoperabilità ed eventuali altre linee guida dell'Agenzia e in caso di parere positivo abilita l'utente all'utilizzo del servizio tracciandone l'attivazione;
3. L'utente abilitato e il richiedente sono informati dell'avvenuta assegnazione del servizio e/o installazione del pacchetto tramite i sistemi ordinari di notifica.

Al fine di garantire la sicurezza e la responsabilità, il processo di abilitazione è tracciato in tutte le sue fasi sul sistema informatico dell'Agenzia ai fini dell'individuazione della responsabilità di processo.

In caso di cessazione dell'utente richiedente i servizi assegnati in precedenza sono revocati.

In caso di cambio di struttura dell'utente richiedente i servizi assegnati in precedenza sono di norma revocati dietro richiesta del responsabile della struttura di provenienza.

5 UTILIZZO DI POSTAZIONI DI LAVORO PERSONALI

La dotazione fornita dall'Agenzia prevede l'utilizzo di computer portatili; pertanto occorre adottare comportamenti adeguati a prevenire l'accesso da parte di soggetti non autorizzati in ragione della:

- natura dei dispositivi: tali dispositivi sono facilmente trasportabili ed occultabili;
- natura dei dati presenti sui dispositivi: sui dispositivi mobili possono essere presenti copie parziali e/o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;
- modalità di utilizzo dei dispositivi: possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Agenzia ed in aree non sicure e ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui ci si riconnette alla rete interna.

5.1 PREVENZIONE E SALVAGUARDIA DEI DATI

Per evitare quindi accessi non autorizzati ai dati e ai servizi dell'Agenzia si raccomanda di:

- non memorizzare in locale, in chiaro, le proprie credenziali che consentano l'accesso alla rete o ad applicazioni dell'Agenzia;
- rendere inintelligibili i dati sensibili e/o giudiziari contenuti i nei supporti rimovibili, impiegando strumenti preventivamente concordati con il SIID;
- non salvare dati in locale, ma utilizzare sempre il cloud o le cartelle di rete, impostando o facendo impostare permessi di accesso adeguati (col criterio del minimo accesso necessario);

- non utilizzare i dischi delle proprie postazioni di lavoro e gli spazi Cloud condivisi o personali per memorizzare software, documenti e più in generale files che esulano dalle proprie finalità lavorative;
- evitare di utilizzare supporti rimovibili non forniti da Arpae;
- limitare lo scambio dati / file e cartelle con user esterni a dominio Arpae solo attraverso strumenti informatici messi a disposizione dal SIID rimuovendo la condivisione al termine del lavoro;
- non lasciare la Postazione di Lavoro incustodita con sessione Windows sbloccata.

5.2 PREVENZIONE E SALVAGUARDIA DELLE POSTAZIONI DI LAVORO PORTATILI

Per prevenire furto, danneggiamento involontario e comunque situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, l'utente è tenuto a:

- custodire adeguatamente i dispositivi anche fuori dall'orario di servizio o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio);
- durante il trasporto osservare le istruzioni del fabbricante per la protezione dei dispositivi da urti, campi elettromagnetici e sbalzi di temperatura;
- trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
- non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;
- non lasciare i dispositivi incustoditi in auto
- non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.

I computer portatili ad uso individuale devono essere utilizzati esclusivamente dall'utente a cui gli stessi sono stati assegnati e, qualora siano assegnati alle strutture, il loro utilizzo deve essere regolamentato dalle stesse, in funzione delle proprie esigenze ed in modo tale da garantire il controllo.

In caso di furto o smarrimento fare immediata denuncia all'autorità competente e darne comunicazione al responsabile SIID ed al DPO di Arpae.

5.3 UTILIZZO DI SMARTPHONE E TABLET FORNITI DALL' AGENZIA

I dispositivi mobili, in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni dell'Agenzia in quanto soggetti a rischi specifici quali perdita di informazioni, accesso a dati "sensibili", facilità di furto, accesso a reti wireless non sicure, possibilità di download di app con contenuto malevolo.

Nei dispositivi mobili assegnati al personale da parte del SIID, nell'ambito della postazione di lavoro, deve essere presente il profilo di lavoro di Google Workspace impostato tramite l'account dell'utente. Questo consente di gestire il dispositivo mobile centralmente tramite uno strumento di Mobile Device Management applicando le policy dell'Agenzia.

Gli smartphone forniti dall'Agenzia per l'assolvimento delle attività istituzionali (comprese le attività di pronta disponibilità) non devono essere collegati ad alcun account personale di Google Workspace e sono assegnati al Dirigente della struttura responsabile dell'attività.

Sullo smartphone o sul tablet aziendale potrà coesistere, con il profilo di lavoro, un profilo personale (sul quale l'Agenzia non può intervenire). In alternativa, l'utente potrà installare anche una SIM personale da gestire nel profilo personale, in modo totalmente indipendente e scollegato dall'uso aziendale.

Le App disponibili nel profilo di lavoro sono presenti in un elenco autorizzato dall'Agenzia aggiornabile su richiesta motivata. Alcune App a valenza aziendale possono essere installate automaticamente da parte degli amministratori di sistema.

Per ridurre il livello di esposizione alle minacce viene stabilito che:

- Ogni utente che riceve in dotazione un dispositivo mobile è responsabile del suo corretto utilizzo e custodia.
- È fatto divieto di effettuare la disinstallazione del profilo di lavoro o disattivazione dell'agente MDM dal dispositivo mobile da parte degli utenti.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'Agenzia, attraverso il sistema MDM, attiva automaticamente l'impostazione del blocco dello schermo per inattività con sblocco attraverso, pin o riconoscimento biometrico.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'Agenzia, attraverso il sistema MDM, installa sul dispositivo mobile un software anti malware il cui database è aggiornato continuamente (database definizione virus).
- L'utente non può installare App che non siano state pre approvate all'interno del profilo di lavoro e allo stesso modo non può disinstallare quelle considerate essenziali dal SIID.
- È fatto divieto di modificare funzionalità del sistema operativo del dispositivo mobile attraverso operazioni di "rooting" o "jailbreaking".
- L'utente è tenuto a mantenere aggiornato il dispositivo, applicando tutte le patch di sicurezza, upgrade del sistema operativo e aggiornamenti delle applicazioni installate.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile, sia all'interno che all'esterno degli uffici Arpae, riponendolo in cassetti o armadi chiusi a chiave in caso di non utilizzo.
- In caso di furto o smarrimento del dispositivo l'utente deve effettuare la denuncia presso le autorità competenti e far pervenire una copia della denuncia al SIID e, qualora non avesse provveduto in autonomia a bloccare e cancellare i contenuti del dispositivo mobile, è tenuto a segnalarlo tempestivamente al servizio SIID, in modo che gli incaricati della gestione dei dispositivi mobili dell'Agenzia provvedano alla cancellazione remota dei dati contenuti all'interno e al blocco del dispositivo;
- Poiché i dispositivi mobili sono utilizzati su reti di cui l'Agenzia non ha nessun controllo, con conseguente rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi, l'utente è invitato ad utilizzare reti Wi-Fi con accesso tramite autenticazione.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'Agenzia è tenuto ad effettuare un audit periodico delle attività effettuate dagli utenti possessori di dispositivi mobili, allo scopo di individuare accessi non autorizzati ai dati, violazioni delle policy e compromissioni dei dispositivi. Tale audit viene effettuato senza alcuna comunicazione preventiva all'utente, nell'interesse della tutela del patrimonio informativo dell'Amministrazione e della sicurezza delle informazioni degli utenti.
- Salvo specifica richiesta dell'Autorità giudiziaria la funzione degli strumenti di MDM che consente il tracciamento della posizione fisica in cui si trova il dispositivo (geo localizzazione), è disattivata.
- Nei dispositivi con doppia SIM è necessario, qualora si proceda a creare un proprio profilo personale, a utilizzare una propria SIM per l'uso dei servizi voce.
- La SIM in dotazione a ciascun utente prevede un tetto massimo di dati utilizzabili su base mensile che viene automaticamente esteso in caso di utilizzo oltre il limite da parte dell'utente.

5.4 LAVORO AGILE

Per le attività in lavoro agile è previsto l'utilizzo della postazione di lavoro personale assegnata all'utente.

Arpae fornisce ai dipendenti che fruiscono del lavoro agile l'attrezzatura tecnologica adatta e necessaria in base alla specifica attività da svolgere e ne garantisce la conformità alle disposizioni vigenti in materia di salute e sicurezza. Ai sensi dell'art. 18, comma 2, della Legge n. 81/2017 l'Amministrazione è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati per lo svolgimento

dell'attività lavorativa.

Ai dipendenti viene fornita la strumentazione che, di norma, prevede un PC notebook, uno smartphone (eventualmente utilizzabile per la connettività) e gli accessori previsti per il comfort lavorativo nelle diverse situazioni (mouse, cuffia con microfono, zainetto per il trasporto della strumentazione).

Il personale si impegna a custodire con la massima cura e a mantenere integra la strumentazione fornita, in modo tale da evitarne il danneggiamento, lo smarrimento e a utilizzarla in conformità con le istruzioni ricevute.

Gli strumenti di lavoro affidati al personale devono essere utilizzati per lo svolgimento dell'attività lavorativa.

5.5 UTILIZZO DEI DISPOSITIVI NON FORNITI DALL'AGENZIA

I soggetti accreditati al dominio Arpae hanno accesso ai servizi dell'Agenzia esposti sulla rete esterna o resi disponibili in modalità cloud, pertanto fruibili attraverso una pluralità di dispositivi.

Al fine di mantenere la sicurezza dei dati di proprietà dell'Agenzia trattati attraverso tali dispositivi è necessario che l'utente adotti gli accorgimenti e gli strumenti necessari per garantire la riservatezza, l'integrità e la disponibilità dei dati memorizzati sull'infrastruttura informatica dell'Agenzia, prevenendone la memorizzazione insicura ovvero la loro trasmissione attraverso una rete insicura, dove possono essere facilmente compromessi. Obiettivo di queste disposizioni è anche la tutela dell'utente stesso, che adottando i comportamenti indicati non incorre in violazioni delle normative vigenti e nel riconoscimento di responsabilità.

L'utente che accede ai servizi aziendali fuori dalla rete Arpae è tenuto a:

- non memorizzare dati dell'Agenzia su dispositivi personali, soprattutto nel caso di documenti classificati come "confidenziali" o "strettamente confidenziali" e nel caso di presenza di dati personali (in particolare se sensibili o giudiziari) e a non scaricare in locale gli allegati di posta elettronica. Nel caso in cui i dati dell'Agenzia venissero inavvertitamente salvati sul dispositivo personale, l'utente è tenuto a cancellarli immediatamente dal dispositivo;
- impostare il blocco automatico dello schermo del dispositivo dopo pochi minuti di inattività (interazione utente-device) con sblocco attraverso password, pin o riconoscimento biometrico;
- installare sul dispositivo un software anti malware con aggiornamento costante del database di definizione dei malware;
- utilizzare in via esclusiva il dispositivo configurato per l'accesso a dati dell'Agenzia, quindi senza condividerne l'utilizzo con altri soggetti, compresi i propri familiari;
- mantenere aggiornato il dispositivo, applicando tutte le patch di sicurezza, upgrade del sistema operativo e aggiornamenti delle applicazioni installate;
- non installare sul dispositivo applicazioni provenienti da fonti non ufficiali e/o potenzialmente pericolose per l'integrità e la sicurezza dei dati dell'Agenzia;
- non utilizzare sul dispositivo lo stesso client per accedere sia alla posta elettronica aziendale che a quella personale ovvero per accedere ai documenti dell'Agenzia disponibili in cloud.

5.6 UTILIZZO DI SMARTPHONE E TABLET PERSONALI PER L'ACCESSO A DATI E SERVIZI DELL'AGENZIA

È possibile accedere ad alcune delle risorse dell'Agenzia a mezzo di smartphone e tablet anche di proprietà personale.

Per questi casi, oltre a quanto già prescritto nel paragrafo precedente, si stabilisce che:

- La configurazione dell'account Google aziendale implica l'accettazione della creazione di una partizione criptata adibita all'attività lavorativa (definito spazio di lavoro) per la gestione avanzata del dispositivo mobile Android.
- Lo spazio di lavoro è protetto forzatamente dal blocco automatico dello schermo dopo pochi minuti di inattività con sblocco attraverso password, pin o riconoscimento biometrico.
- Come indicato nel paragrafo precedente l'utente è tenuto ad installare sul proprio dispositivo mobile un software antimalware.
- L'utente è tenuto a non installare app al di fuori dei canali di distribuzione ufficiali (Google Play, Microsoft Store o Apple Store) e a non installare app non compatibili con la sicurezza dei dati.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile. L'utente deve, inoltre, effettuare la denuncia presso le autorità competenti e far pervenire una copia della denuncia al SIID.
- Nel caso in cui l'utente sospetti una violazione dei dati dell'Agenzia, la presenza di un malware, oppure la compromissione del proprio dispositivo mobile personale utilizzato per accedere a dati dell'Agenzia, è tenuto a segnalarlo tempestivamente all'assistenza utenti del SIID, in modo che, se fosse confermata una compromissione di dati dell'Agenzia, possano essere attivate opportune contromisure al fine di limitare i danni.
- Poiché i dispositivi mobili sono utilizzati su reti di cui l'Agenzia non ha nessun controllo, esiste un rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi. Per tali motivi l'utente è invitato ad utilizzare preferibilmente reti Wi-Fi con accesso tramite autenticazione.

6 UTILIZZI DELLA RETE ARPAE

Al fine di prevenire l'accesso ai sistemi informatici da parte di soggetti non autorizzati è fatto divieto di:

- connettere ad Internet, tramite reti wi-fi, modem o altri apparati di accesso remoto non espressamente autorizzati, strumentazioni informatiche collegate alla rete interna dell'Agenzia;
- connettere alla rete interna dell'Agenzia strumenti elettronici personali o comunque non espressamente autorizzati;
- connettere alla rete interna dell'Agenzia access point o altri apparati di rete non espressamente autorizzati;
- installare e/o comunque utilizzare software peer-to-peer o utilizzare le postazioni di lavoro collegandole tra loro per la condivisione di file e stampanti;
- utilizzare strumenti di sniffing, cracking o scanning e introdurre o diffondere volontariamente programmi nocivi nella rete o nei sistemi.

7 POSTA ELETTRONICA

La casella di posta elettronica viene fornita dall'Agenzia quale strumento di supporto per lo svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa.

Le caselle di posta elettronica sono assegnate come servizio di base a ciascun dipendente e collaboratore al momento dell'instaurazione del rapporto di lavoro/collaborazione.

Ai collaboratori esterni accreditati al dominio Arpae la casella di posta è assegnata su richiesta motivata del Responsabile della struttura qualora risulti indispensabile per svolgere attività che non risulta possibile svolgere con email personali e/o aziendali.

L'attivazione di ulteriori caselle di posta elettronica, per attività di gruppo o di progetto, può essere richiesta al SIID dal Responsabile di struttura o da un suo delegato.

Eccezionalmente al fine di assicurare la disponibilità dei dati e delle informazioni pervenute o inviate dalle

caselle di posta elettronica è prevista la creazione e l'utilizzo di caselle di posta elettronica di struttura e/o di Gruppo condivise tra gli utenti che concorrono alle suddette attività.

L'amministrazione degli utenti che accedono a caselle di struttura, di gruppo o di progetto è assegnata nominalmente.

La casella di posta elettronica personale rientra tra gli strumenti di lavoro assegnati agli utenti.

L'accesso al contenuto della casella di posta elettronica personale è consentito solo all'utente assegnatario. L'accesso da parte di terzi alla casella personale di un utente è vietato salvo quanto indicato nel paragrafo 14. È inoltre fatto salvo l'eventuale accesso disposto a richiesta dell'Autorità giudiziaria.

Le caselle di posta elettronica certificata (PEC) non sono di norma nominative, ma assegnate alle strutture Arpae per le quali sono previsti processi di comunicazione istituzionale con soggetti terzi. Solo in casi particolari e documentati possono essere richieste al SIID PEC nominative.

7.1 UTILIZZO DELLA POSTA ELETTRONICA

La posta elettronica deve essere utilizzata per le specifiche finalità della propria attività lavorativa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi e degli altri utenti di Arpae e dei processi lavorativi, adottando comportamenti idonei a prevenire la perdita di confidenzialità di dati riservati e l'utilizzo non appropriato di beni dell'Agenzia.

La casella di posta elettronica certificata (PEC) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali. Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione costituisce comunicazione di dati personali e, come tale deve essere effettuata ai sensi della normativa vigente, oppure a riscontro di una istanza dell'interessato ai propri dati personali.

Nel caso di utilizzo della posta elettronica certificata (PEC) per la trasmissione di dati personali comuni (vale a dire non sensibili e/o giudiziari) il cui trattamento sia di titolarità dell'Agenzia, l'utente dovrà solo accertarsi della legittimità del destinatario a ricevere i dati personali che intende inviare; qualora venisse utilizzata, invece, la casella di posta elettronica "ordinaria" l'utente dovrà accertarsi, oltre che della legittimità del destinatario alla ricezione dei dati personali, anche dell'identità dello stesso, che si intende certa se:

- ha presentato via email una richiesta per l'invio dei dati firmata digitalmente;
- ha inviato, oltre alla richiesta di dati presentata via email o telefonicamente, anche una copia semplice di un documento di identità in corso di validità (anche tramite email).

Nel caso di ragionevole certezza sull'identità del richiedente (ad esempio perché il richiedente è conosciuto personalmente) ovvero in casi di improrogabile urgenza, l'accertamento dell'identità del ricevente può essere effettuata per via telefonica.

Le modalità tecniche cambiano in relazione alla tipologia dei dati personali che si intende inviare.

Nei casi in cui sia necessario inviare dati personali sensibili e/o giudiziari, rilevata da parte dell'utente la liceità del trattamento ai sensi della normativa vigente, la comunicazione deve essere effettuata utilizzando la modalità "riservata" se prevista dal fornitore del servizio di posta in cloud.

Per proteggere i dati sensibili dagli accessi non autorizzati, si possono inviare messaggi e allegati con la modalità riservata di Gmail che consente di impostare una data di scadenza per i messaggi o revocare l'accesso in qualsiasi momento. Per i destinatari del messaggio riservato saranno disattivate le opzioni di inoltro, copia, stampa e download.

Anche se la modalità riservata serve a impedire che i destinatari condividano per errore la email ricevuta, non impedisce loro di realizzare screenshot o foto dei messaggi o dei loro allegati. Se i destinatari hanno programmi dannosi sul computer, potrebbero comunque essere in grado di copiare o scaricare i messaggi o gli allegati.

7.2 SUGGERIMENTI PER LA PREVENZIONE DA MALWARE

Al fine di prevenire le minacce rappresentate da software malevoli (per es. virus, ransomware, spyware, worm ecc.) che potrebbero essere contenuti in email o negli allegati delle email stesse, si forniscono le seguenti indicazioni:

1. "*Spam*" è il termine con cui si indica l'invio incessante, ma soprattutto indesiderato, di messaggi ad un gran numero di utenti contemporaneamente. Le operazioni di invio possono realizzarsi via email o tramite i gruppi di discussione. A titolo preventivo si raccomanda di:
    - non rispondere mai a messaggi di presunto spam, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
    - limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail su siti web pubblici (per es. forum, mailing list, ecc.);
    - non fare click sui collegamenti eventualmente contenuti nei testi delle comunicazioni;
    - evitare di scaricare eventuali allegati;
    - non rispondere o inoltrare email di c.d. "Catene di S. Antonio", ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
    - non configurare la conferma di lettura in modalità automatica qualora questa sia consentita nell'ambito del sistema di posta elettronica dell'Agenzia.

2. Il "*phishing*" è una tecnica di attacco che sfrutta email e siti web contraffatti del tutto simili nell'aspetto agli originali, per ingannare l'utente e carpire informazioni confidenziali o personali. È necessario, quindi, prestare massima attenzione alle email che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di corrieri ecc.).

In caso di dubbi sulla qualità di messaggi email, si raccomanda di contattare il SIID.

8 FIRMA ELETTRONICA

Ad ogni dipendente ARPAE viene rilasciato, senza oneri, un kit di firma qualificata eIDAS remota con generazione dell'OTP tramite una app installata sullo smartphone di servizio. La firma digitale deve essere utilizzata dal dipendente per le attività lavorative assegnate e resta nelle disponibilità del dipendente che potrà continuare ad utilizzarla anche in caso di interruzione a titolo definitivo del rapporto di lavoro con Arpae. La firma digitale può essere utilizzata dal dipendente anche in ambito non lavorativo solo qualora la firma rilasciata non riporti l'indicazione di ARPAE Emilia-Romagna quale organizzazione di appartenenza del dipendente.

9 NAVIGAZIONE IN INTERNET

L'Agenzia fornisce l'accesso ad Internet a supporto dello svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa e per questo se ne prescrive un utilizzo pertinente alle specifiche finalità, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.

È fatto divieto di:

- modificare le configurazioni standard dei browser web forniti dall'Ente;
- accedere a caselle web mail di posta elettronica personale forniti da provider che non assicurano strumenti di protezione adeguati;
- scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, verificare la provenienza e l'autenticità del software (per es. tramite meccanismi di firma digitale);
- utilizzare siti pubblici di condivisione dei file e di archiviazione online forniti da provider che non assicurano strumenti di protezione adeguati;
- caricare documenti inerenti l'attività lavorativa o istituzionale, soprattutto se contenenti dati personali, sensibili e/o giudiziari, su siti pubblici di condivisione, archiviazione o backup online;
- utilizzare siti che permettano di usufruire di web proxy pubblici, aggirando l'obbligo di utilizzo del web proxy dell'Agenzia per la navigazione;
- collegarsi a URL o servizi ed eseguire il download di materiale estraneo ai fini lavorativi (quali libri, immagini, filmati, file audio non inerenti alla propria attività lavorativa) e in modo particolare materiale protetto da copyright senza adeguato pagamento dei diritti d'autore o materiali che violi le leggi vigenti

Viste le nuove tipologie di attacco che hanno sempre più per oggetto l'utente finale e come mezzo di propagazione il web o la posta elettronica, e visto che sempre più le comunicazioni web utilizzano canali cifrati, il personale del SIID addetto alla sicurezza informatica è autorizzato a configurare i sistemi di sicurezza dedicati alla navigazione web affinché venga ispezionato il traffico cifrato per alcuni siti ritenuti ad alto rischio, tipicamente quelli che permettono lo scambio di documenti, allo scopo di individuare e bloccare eventuale malware o strumenti di attacco. Tale ispezione è funzionale unicamente alla verifica della sicurezza delle informazioni, è effettuata con strumenti automatici e non comporta alcuna forma di controllo dell'attività lavorativa.

10 PROTEZIONE ANTIMALWARE

L'utente utilizzatore delle risorse informatiche dell'Agenzia è tenuto ad adottare le necessarie cautele al fine di ridurre il rischio di infezione della propria o altrui postazione di lavoro. È fatto quindi divieto, ai soggetti che sono amministratori di postazione di lavoro, di rimuovere il programma antivirus installato su di essa e di alterarne la configurazione. Si invitano gli utenti a segnalare al SIID eventuali problemi eventualmente riscontrati sulla corretta installazione e funzionamento del programma antivirus installato sulla propria postazione di lavoro.

E' vietato collegare al proprio dispositivo supporti rimovibili quali dispositivi di archiviazione non forniti dall'Agenzia e si raccomanda, inoltre, prima di utilizzare supporti rimovibili forniti da Arpae, di verificare la presenza di eventuali malware in esso contenuti.

A seguito di segnalazione della presenza di un malware da parte del software antivirus si prescrive di:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'evento al SIID;
- non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti.

11 GESTIONE DEI LOG

I sistemi informativi dell'Agenzia sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti, ed in particolare dei requisiti di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.

Alcune attività dell'utenza sono soggette a *logging*: ciò significa che alcune operazioni eseguite dagli utenti di sistemi informativi vengono memorizzate in formato elettronico e conservate per un certo periodo di tempo. Il *logging* è necessario per ragioni di sicurezza: il livello del *logging* dei diversi servizi, ossia il livello di dettaglio dei dati memorizzati, è funzionale unicamente alla verifica della sicurezza con la quale i servizi sono erogati e per nessun motivo viene utilizzato per il controllo dell'attività lavorativa.

Di seguito vengono dettagliate le tipologie di log raccolti e conservati:

- log della navigazione web, del firewall e del server di posta: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log delle segnalazioni ed alert di tutte le tipologie provenienti dal sistema antimalware: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli amministratori di sistema ai sistemi amministrati: tale raccolta è motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema;
- log degli accessi degli utenti ai servizi di rete: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli utenti al sistema di stampa e delle operazioni effettuate: tale raccolta deriva dalla necessità di poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log delle attività svolte da utenti e amministratori di sistema nell'ambito di alcuni software complessi: tale raccolta è motivata dalla necessità di poter individuare anche a posteriori eventuali violazione delle policy e audit sulla correttezza dei dati gestiti dal software stesso.

Il tempo di conservazione dei log relativi alla navigazione e dei log del sistema antimalware è di 3 mesi.

Ciò è motivato dalla necessità di utilizzare tali log per la verifica annuale delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema e di avere una policy di retention dei log uniforme per tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.

12 PREVENZIONE E GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Al fine di prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile è fondamentale operare tempestivamente e in uno spirito di collaborazione.

Qualora si ravvisassero violazioni di sicurezza interna o eventi che possano portare a credere che vi sia stata una elusione delle misure di sicurezza previste, è di fondamentale importanza segnalare tempestivamente l'accaduto al SIID.
In un'ottica di prevenzione degli incidenti di sicurezza, è necessario attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna dell'Agenzia.

13 PROTEZIONE DEI DATI TRATTATI SENZA L'UTILIZZO DI STRUMENTI ELETTRONICI

L'accesso ai dati trattati senza l'utilizzo di strumenti elettronici è consentito, come per i trattamenti di dati personali
effettuati con mezzi elettronici, esclusivamente al personale espressamente incaricato.

Vi sono, inoltre, alcuni basilari comportamenti che, se messi in atto, riducono in maniera considerevole i rischi di accesso ai dati da parte di persone non autorizzate, di perdita di confidenzialità dei dati e della conseguente mancanza di disponibilità degli stessi.

In linea con ciò, risulta, ad esempio, assolutamente necessario raccogliere prontamente, nel caso di utilizzo di stampanti di rete o fax ubicati in locali comuni (per es. corridoi), i documenti stampati, soprattutto se contenenti dati personali, in modo da preservarne la riservatezza del contenuto. È ugualmente rilevante, ai fini della
tutela dei dati personali trattati nell'espletamento delle proprie funzioni, assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo dell'Ente, non siano lasciati a vista sulla scrivania ma conservati in cassetti o armadi. Conseguentemente e al fine di non eludere tali precauzioni, è opportuno conservare, con le dovute cautele, le chiavi utilizzate per i cassetti e gli armadi contenenti, dati personali e sensibili/giudiziari. In particolare, è utile prevedere opportuni meccanismi per garantire, se necessario, ai propri colleghi la disponibilità delle stesse anche durante periodi di assenza dall'attività lavorativa (per es. copia delle chiavi depositate in segreteria, registro di presa in carico delle chiavi, ecc.).

14 RECUPERO DEI DATI DA PARTE DELL'ENTE IN ASSENZA DELL'UTENTE E INDICAZIONE DEL FIDUCIARIO

In questo paragrafo sono individuate apposite procedure volte a:

A. permettere all'Ente di recuperare dati, informazioni o documenti trattati nell'espletamento delle attività lavorative di un dipendente o un collaboratore, nei casi in cui l'assenza dello stesso sia programmata (ad esempio per ferie) oppure sia improvvisa e imprevista (ad esempio per malattia);
B. abilitare altri collaboratori (ad es. gli addetti ad una segreteria) all'utilizzo della casella di posta elettronica pur

in presenza del titolare della casella stessa (ad es. il dirigente di struttura).

Nel caso di cui alla lettera A), tali procedure sono volte a bilanciare il diritto dell'Ente a garantire l'operatività organiz-
zativa e amministrativa e l'uso consono degli strumenti forniti agli utenti con il diritto del lavoratore alla tutela della
propria sfera di riservatezza anche nell'ambito della propria attività lavorativa.

Nel pieno rispetto del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" e degli orientamenti sia del Garante stesso sia giurispruden-
ziali in materia, con le procedure di seguito esplicitate sono disciplinati in maniera esaustiva i casi in cui i dati relativi
all'attività lavorativa del dipendente e del collaboratore possano essere conosciuti dall'Ente nell'esercizio delle proprie prerogative organizzative. La priorità è concessa a modalità e strumenti che non comportano un accesso diretto ai dati personali e alle informazioni trattate dall'utente e quindi a funzionalità che meno comprimono il diritto alla riservatezza.

In accoglimento delle indicazioni ricevute dal Garante con il Provvedimento suindicato, figura centrale delle procedure di seguito specificate è il "fiduciario". Questi è un soggetto scelto liberamente da ciascun utente, che ha il compito di assicurare l'accesso ai dati trattati dall'utente fiduciante solo nei casi di assenza dello stesso. Quest'ultimo è ovviamente tenuto ad avvisare preventivamente il fiduciario e a comunicarne l'indicazione nominativa al Dirigente della Struttura di appartenenza. A titolo esemplificativo il "fiduciario" potrebbe essere un collega che collabora nello stesso settore di attività lavorativa del fiduciante oppure che conosce o partecipa a un determinato progetto insieme al fiduciante stesso.

Negli altri casi, qualora l'utente non abbia designato un proprio "fiduciario" e/o non abbia attivato alcuna funzione di delega all'accesso, la possibilità di accedere a suoi messaggi di posta oppure a files o cartelle presenti nello spazio cloud personale, può avvenire soltanto in casi di effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa. Soltanto in tale caso di emergenza sono previste e di seguito esplicitate le procedure che contemplano l'accesso alla casella di posta elettronica e ai dati dello spazio personale dell'utente su istanza del Responsabile della Struttura di appartenenza e per mezzo del personale del SIID.
È comunque fatto divieto allo stesso fiduciario o ad altro utente eventualmente delegato o autorizzato di accedere ai messaggi di posta elettronica e a file o cartelle che, già dall'oggetto e/o dalla denominazione e/o dalle proprietà, possano far prefigurare un contenuto riconducibile a informazioni personali non riconducibili ad attività lavorativa che, anche in tale sede, devono ricevere la dovuta tutela.

È fatto divieto di conservare cartelle e documenti di lavoro sui dischi locali dei personal computer, dei portatili e di smartphone e tablet. Ciò comporterebbe, altrimenti, l'assunzione di rischi elevati in termini di confidenzialità, integrità e disponibilità dei contenuti prodotti da ciascun utente e, pertanto, deve essere limitata a operazioni su copie temporanee di lavoro.

Ogni utente ha a disposizione spazi di conservazione in cloud, eventualmente replicati e sincronizzati sul proprio dispositivo locale, ai fini di conservare documenti e bozze di lavoro; tale tecnologia garantisce

backup, recupero di cancellazioni errate, gestione delle versioni e controlli di sicurezza.

Nei casi in cui l'Ente abbia necessità di accedere a contenuti necessari ad assicurare la continuità dell'attività lavorativa che l'utente abbia incautamente memorizzato sul disco locale della postazione di lavoro assegnata, si applicano per analogia le regole stabilite nei paragrafi seguenti.

14.1 RECUPERO DATI IN CASO DI ASSENZE PROGRAMMATE

In caso di assenze programmate (ad esempio in caso di ferie) e qualora vi siano esigenze di assicurare la continuità
dell'attività lavorativa, l'utente condivide:

- l'accesso in delega ai propri messaggi di posta elettronica a mezzo del software in utilizzo
- file o cartelle a mezzo del cloud

in favore del proprio fiduciario oppure in favore di altro soggetto, (ad es. quando lo stesso fiduciario è assente).
Il fiduciario o comunque il soggetto delegato farà accesso ai soli messaggi di posta elettronica o file/cartelle necessari
ad assicurare la continuità dell'attività lavorativa.
Lo stesso "fiduciario" (o il delegato) può comunicare ai mittenti dei messaggi ricevuti nella casella di posta dell'utente assente, l'assenza dell'utente "fiduciante", e che, sino ad una determinata data, sarà lui stesso a prendere visione dei messaggi inviati su quella casella di posta.

14.2 RECUPERO DATI IN CASO DI ASSENZE NON PROGRAMMATE CON INDICAZIONE DEL FIDUCIARIO

In caso di assenze non programmate, come ad esempio per malattia, e qualora l'utente non abbia attivato le funzioni
di condivisione descritte nel paragrafo precedente, il Responsabile della Struttura di appartenenza dell'utente assente, esclusivamente per effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa, può richiedere al Responsabile del SIID di attivare la funzione di delega all'accesso alla casella di posta elettronica o al cloud assegnato all'utente assente.

La funzione di delega sarà attivata in favore dell'utente eventualmente designato preventivamente quale "fiduciario" dall'utente assente.
L'istanza di accesso deve essere trasmessa anche in copia all'utente assente e al fiduciario dallo stesso nominato. La funzione di delega su descritta rimane attiva per il tempo strettamente necessario al recupero dei contenuti e delle informazioni che si reputano indispensabili per dare continuità all'attività lavorativa dell'Ente oppure per un periodo di tempo limitato (quale ad esempio quello della malattia dell'utente assente) al termine del quale la funzione di delega è automaticamente disattivata.

14.3 RECUPERO DATI IN CASO DI ASSENZE CON MANCATA INDICAZIONE DEL FIDUCIARIO

Qualora l'utente assente non avesse provveduto a individuare un proprio "fiduciario" e non avesse delegato neppure altri soggetti ad accedere ai propri contenuti, si prevede, sia nel caso in cui l'assenza sia programmata sia nel caso in cui non lo sia, che:

a) il Responsabile della Struttura di appartenenza dell'utente assente che, esclusivamente per le succitate esigenze intende accedere a messaggi (inclusi gli eventuali allegati) presenti nella casella di posta elettronica o a file/cartelle presenti nel cloud assegnato allo stesso, deve effettuare la richiesta al

Responsabile del SSIID;

b) l'accesso può essere autorizzato esclusivamente al personale del SIID che viene designato incaricato del trattamento di dati personali che sia strettamente necessario effettuare al fine di adempiere ai compiti assegnatigli con l'istanza di cui alla lettera a);

c) è fatto divieto al personale del SIID di accedere ai messaggi di posta elettronica o file/cartelle che, già dall'oggetto,
possano far prefigurare un contenuto riconducibile a informazioni personali non relative all'attività lavorativa
del soggetto assente; la funzione di delega descritta rimane attiva per il tempo strettamente necessario al recupero dei contenuti che si reputano indispensabili per dare continuità all'attività lavorativa oppure per un periodo di tempo predeterminato (quale ad esempio quello della malattia dell'utente assente) al termine del quale la funzione viene automaticamente disattivata.

14.4 AUTORIZZAZIONE ALL'UTILIZZO DELLA CASELLA DI POSTA ELETTRONICA AD ALTRI COLLABORATORI

Nel caso in cui un utente reputasse opportuno, al fine di organizzare in maniera più efficiente la propria attività lavorativa, autorizzare ulteriori collaboratori (esempio gli addetti alla Segreteria) all'utilizzo della propria casella di posta elettronica, calendario, attività, note, e contatti può utilizzare le funzioni di delega previste dall'applicativo di posta elettronica.

15 Sicurezza e PROTEZIONE DEI DATI

Il legame tra lavoratore ed azienda si basa su un rapporto contrattuale e su obblighi di tipo normativo che l'azienda deve assolvere nei confronti della persona che ha assunto.

Durante la vita lavorativa il lavoratore potrà venire a conoscenza di una varietà di dati personali riferiti a persone interne od esterne ad Arpae, dati che può o deve trattare per le necessità amministrative dell'ente e per la gestione del rapporto lavorativo. I dati andranno dai più comuni dati anagrafici a cosiddetti dati sensibili, ovvero indicatori di uno stato di salute (es. malattie, permessi di cui alla L. n. 104/1992, idoneità al lavoro), di origini etniche e razziali (es. permesso di soggiorno) e di orientamento/vita sessuale (es. certificato di matrimonio, bonus famiglia ecc.), o dati giudiziari.
Il trattamento dei dati comuni si poggia su più basi giuridiche, diverse a seconda della categoria di dato oggetto di elaborazione. Per i dati personali comuni (dati anagrafici, coordinate bancarie ecc.) il trattamento trova fondamento nell'esecuzione del contratto di lavoro in essere tra le parti, e negli obblighi normativi (es. contabili e fiscali) cui è soggetta l'azienda. Per queste tipologie di trattamenti il GDPR identifica due basi giuridiche ben chiare e distinte all'articolo 6 comma 1 lettere b) e c), rispettivamente trattamenti derivanti da attività contrattuali e da obblighi di legge.
Premesso ciò, il dipendente ha l'obbligo di osservare, nello svolgimento della propria prestazione lavorativa, un comportamento di massima tutela e riservatezza della privacy ed osservare tutte le misure necessarie alla protezione dei dati nel rispetto del Regolamento UE n. 679/2016 e del D.lgs. n. 196/2003 e successive modifiche e integrazioni.
In particolare:

1. I/le lavoratori/lavoratrici stessi mantengono l'obbligo di custodire con la massima diligenza la strumentazione tecnologica assegnata, sia Hardware sia Software, di mantenere integra la strumentazione fornita, in modo tale da evitarne il danneggiamento, lo smarrimento e ad utilizzarla in conformità con le istruzioni ricevute. In caso di furto o smarrimento delle dotazioni hardware assegnate, il/la dipendente dovrà presentare apposita denuncia all'autorità di pubblica sicurezza, e darne avviso al proprio dirigente, per la richiesta di sostituzione e per l'inoltro delle dovute comunicazioni ai fornitori (in caso di apparecchiature a noleggio) o alle compagnie assicuratrici (in caso di apparecchiature in proprietà Arpae). Gli strumenti di lavoro affidati al personale devono essere utilizzati per lo svolgimento dell'attività lavorativa; possono essere utilizzati per finalità diverse, ma solo ed esclusivamente con le modalità e nel rispetto di quanto previsto nella presente policy
2. I/le lavoratori/lavoratrici sono chiamati/e a tenere una condotta particolarmente diligente a tutela dei dati trattati. Hanno, altresì, il dovere di riservatezza ed il divieto di diffusione non autorizzato su tutte le informazioni delle quali vengano in possesso per il lavoro assegnato e di quelle derivanti dall'utilizzo dei programmi e dei dati in essi contenuti.
3. Il/la lavoratore/lavoratrice dovrà tempestivamente informare il/la responsabile e il DPO (dpo@arpae.it) nel caso in cui si verifichi – nell'ambito della sua attività – una violazione (data breach ai sensi degli artt. 33 e 34 GDPR) dei dati personali oggetto di trattamento che ponga a rischio i diritti e le libertà delle persone fisiche.

L'Amministrazione rende accessibile al/alla lavoratore/lavoratrice tutte le informazioni e i documenti necessari all'esecuzione delle proprie mansioni, rimanendo comunque onerata della protezione degli stessi ed adotta misure e soluzioni tecniche idonee a prevenire la perdita e/o la diffusione dei dati, tanto nel rispetto dei principi di riservatezza nei confronti del/della lavoratore/lavoratrice quanto a tutela dei propri interessi aziendali. Le principali soluzioni adottate, in aggiunta ad idonee iniziative formative, sono: VPN (Virtual Private Network), Cloud (Cloud Computing), ACL (Access Control List), finalizzate a limitare, in particolare, il rischio di accesso non autorizzato, diffusione, perdita e distruzione dei dati.

Il lavoratore che accede con la propria utenza ai sistemi informatici di Arpae è autorizzato al trattamento dei dati a cui accede con l'obbligo di osservare le disposizioni in materia di tutela e trattamento dei dati personali, secondo quanto previsto nei vigenti codici di comportamento e nella normativa di riferimento.

Il lavoratore, quale autorizzato al trattamento, si impegna pertanto ad osservare le seguenti modalità operative per il trattamento dei dati.

1. richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa;
2. custodire i dati oggetto del trattamento in luoghi non accessibili a non autorizzati;
3. non lasciare incustodito il proprio posto lavoro prima di aver provveduto alla messa in sicurezza dei dati;
4. non lasciare incustoditi e accessibili a terzi gli strumenti elettronici, mentre è in corso una sessione di lavoro;
5. procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni di consultazione;
6. custodire e non divulgare il codice di identificazione personale (username) e la password di accesso agli strumenti elettronici;
7. accertarsi che i terzi siano a conoscenza e abbiano autorizzato l'uso dei dati richiesti;
8. accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
9. non fornire telefonicamente o a mezzo email dati senza specifica autorizzazione e/o identificazione del richiedente.

16 RUOLI E RESPONSABILITÀ

Al controllo del rispetto delle procedure, dei divieti e dei comportamenti degli utenti concorrono i seguenti ruoli e responsabilità:

Ruolo / Funzione	**Responsabilità**
Dirigente del Servizio Sistemi Informativi	Adeguare i contenuti della policy in applicazione delle disposizioni normative vigenti nel tempo e avuto riguardo all'evoluzione normativa e tecnologica.
Titolari degli incarichi di funzione preposti allo svolgimento di attività che hanno al loro interno riferimenti alla sicurezza informatica	Adeguare i contenuti della policy in applicazione delle disposizioni normative vigenti nel tempo e avuto riguardo all' evoluzione normativa e tecnologica.
Personale SIID	Responsabile delle procedure di accreditamento e del rilascio delle credenziali informatiche. Responsabile delle procedure di accesso ai fiduciari e delegati sui servizi di posta e dati in cloud. Responsabile della verifica del rispetto delle disposizioni contenute nella presente policy con riferimento al corretto utilizzo delle postazioni di lavoro e delle dotazioni software personali.
Responsabili di struttura	Responsabile del riconoscimento "de visu" e della richiesta di accreditamento degli utenti esterni. Proroga e/o revoca dell'accreditamento ad un utente esterno. Approvazione della richiesta di assegnazione di nuove risorse del sistema informativo/informatico regionale ad un utente accreditato con le procedure di cui alla presente policy. Richiesta di revoca di risorse del sistema informativo/informatico regionale ad un utente accreditato. Diffusione e presa visione a tutti i propri collaboratori dei contenuti del presente documento. Valutazione della strumentazione da concedere in uso ad utenti esterni. Recupero della strumentazione assegnata a collaboratori e dipendenti della propria struttura al termine del periodo di collaborazione
Utenti	Rispetto delle disposizioni contenute nella presente policy.
Personale del Servizio SIID	Disporre procedure e/o soluzioni tecnologiche finalizzate a forzare il corretto rispetto da parte degli utenti delle disposizioni contenute nella presente policy. Effettuare un monitoraggio periodico della rete, dei

	dispositivi di sicu- rezza e delle postazioni di lavoro, al fine di individuare accessi non autorizzati ai dati, violazioni delle policy e compromissioni dei dispositivi. Tale monitoraggio viene effettuato senza alcuna comunicazione preventiva agli utenti, nell'interesse della tutela del patrimonio informativo dell'Amministrazione e della sicurezza delle informazioni degli utenti.

La violazione delle disposizioni contenute nella presente policy, ferme restando eventuali responsabilità penali, civili o amministrativo-contabili, è rilevante sotto il profilo disciplinare e di responsabilità dirigenziale.

17 GLOSSARIO

Termine/Acronimo	Descrizione
Analisi forense	insieme di tecniche rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova.
Autenticazione	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente che accede ai sistemi informativi.
Black List di Reputation	insieme di indirizzi (IP, mail) ai quali, sulla base dei comportamenti tenuti precedentemente (es. invio di spam), è impedito l'utilizzo di alcuni servizi informatici.
Cracking (strumenti di)	software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.
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.
Dati personali	qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
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.
Identificazione informatica	la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza

	dell'accesso.
Dispositivo mobile	sistema di elaborazione che può essere spostato e trasportato. Nel contesto della presente policy, per dispositivo mobile si intende solo “smartphone” o “tablet”, mentre negli altri casi si parla esplicitamente di “computer portatile”, o “postazione di lavoro portatile”
Evidenza	nell’ambito dell’analisi forense, si intende una “traccia” di reato; la raccolta delle evidenze rappresenta una fase della gestione degli incidenti di sicurezza informatica, anche quando non siano presenti implicazioni legali.
Incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
Jailbreaking	Il jailbreak è un termine che indica una procedura che rimuove le restrizioni software imposte da Apple nei dispositivi iOS. Permette di installare software e pacchetti di terze parti, non firmati e autorizzati da Apple, alternativi a quelli dell'App Store.
Malware	Termine generico che indica software dannosi progettati per compromettere o sfruttare qualsiasi tipo di dispositivo, servizio o rete programmabile.
Password	sequenza di caratteri alfanumerici che costituisce la chiave d'accesso ad un sistema protetto. In assenza di altri dispositivi, la password costituisce il meccanismo di sicurezza base per la protezione dell’accesso a risorse informatiche.
Patch	aggiornamento di un software per la correzione di un problema di sicurezza o di funzionalità.
Peer-to-peer (strumenti)	software che permettono l'utilizzo di una postazione di lavoro in modalità server per consentire lo scambio di file con altri utenti, anche esterni alla rete dell'Ente.
Phishing	tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).
Postazione di lavoro (PdL)	Il pc o il portatile comprensivo di tutte le periferiche di input e output (mouse, tastiera, webcam, video, stampante collegata) che costituiscono la dotazione hardware assegnata ad un utente.
Ransomware	tipo di malware che limita l'accesso del dispositivo che infetta (per esempio cifrando i dati), chiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione
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.
Rooting	Il rooting è un processo informatico che permette agli utenti di smartphone, tablet o altri dispositivi dotati di sistema operativo Android di ottenere controlli privilegiati su vari sottosistemi Android.
Scanning	attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.
Sniffing (strumenti di)	software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.
Spamming	l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.

Spyware	software che raccoglie informazioni riguardanti un utente senza il suo consenso, inviandole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.
Supporto rimovibile	dispositivo su cui è possibile registrare dati che può essere facilmente rimosso dal sistema che lo legge/scrive, trasportato in altri luoghi e collegato ad altri sistemi. Esempi di supporti rimovibili sono: chiavette USB, hard disk esterni, CD ROM.
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.
Worm	programma in grado di auto diffondersi sulla rete e verso altri sistemi.
Virus	programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.