ARPAT
Agenzia regionale per la protezione ambientale della Toscana

Decreto del Direttore generale nr. 171 del 28/12/2017

Proponente: *Marco Chini*

Sira

Pubblicità/Pubblicazione: Atto soggetto a pubblicazione integrale (sito internet)

Visto per la pubblicazione - Il Direttore generale: Ing. Marcello Mossa Verre

Responsabile del procedimento: *Dott. Marco Chini*

Estensore: *Mario Daddi*

Oggetto: Settore SIRA - Disciplinare ICT e trattamenti dati - Revisione 01 (Disciplinare sull'utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati), Politica ICT e trattamenti dati - Revisione 00

ALLEGATI N.: 2

Denominazione	*Pubblicazione*	*Tipo Supporto*
Allegato A "Disciplinare ICT e trattamenti dati - Revisione 01"	Si	digitale
Allegato B "Politica ICT e trattamenti dati - Revisione 00"	Si	digitale

Natura dell'atto: *immediatamente eseguibile*

Il Direttore generale

Vista la L.R. 22 giugno 2009, n. 30 e s.m.i., avente per oggetto "Nuova disciplina dell'Agenzia regionale per la protezione ambientale della Toscana (ARPAT)" ;

Richiamato il decreto del Presidente della Giunta Regionale n. 22 del 28.02.2017, con il quale il sottoscritto è nominato Direttore generale dell'Agenzia Regionale per la Protezione Ambientale della Toscana;

Dato atto che con decreto del Direttore generale n. 238 del 13.09.2011 è stato adottato il Regolamento di organizzazione dell'Agenzia (approvato dalla Giunta Regionale Toscana con delibera n. 796 del 19.09.2011), successivamente modificato con decreti n.1 del 04.01.2013 e n. 108 del 23.07.2013;

Visto l'"Atto di disciplina dell'organizzazione interna" approvato con decreto del Direttore generale n. 270/2011 (ai sensi dell'articolo 4, comma 3, del Regolamento organizzativo dell'Agenzia), modificato ed integrato con decreti n. 87 del 18.05.2012 e n. 2 del 04.01.2013;

Visto il Regolamento (UE) 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016, noto come GDPR, che modifica la normativa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Visto l'art. 17 del D.Lgs. n. 82 del 07/03/2005, noto come Codice dell'amministrazione digitale (CAD), aggiornato con D.Lgs. n. 179 del 26/08/2016, che stabilisce l'obbligo, per le pubbliche amministrazioni di:

- garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche di cui all'articolo 71 del CAD;
- affidare a un unico ufficio dirigenziale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
- di attribuire al suddetto ufficio i compiti analiticamente descritti al medesimo art.17;

Vista la Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri, che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale;

Visto l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" contenuto nella Circolare 18 aprile 2017, n. 2/2017 di AgID, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicato in Gazzetta Ufficiale (Serie Generale n.103 del 5/5/2017);

Considerato che

1. la gestione delle risorse ICT e dei trattamenti dati effettuati in ARPAT è regolamentata da:
    - "Documento programmatico della sicurezza (DPS)", approvato con Decreto D.G. n. 163 del 29.3.2006 e successivamente aggiornato con i Decreti D.G. n. 214 del 5.5.2006, n. 141 del 30.4.2007, n. 76 del 31.3.2008, n. 147 del 28.4.2009, n. 149 del 31.3.2011;
    - Disciplinare ICT e trattamenti dati" Revisione 00, approvato con Decreto D.G. n. 147 del 28.4.2009, che regolamenta l'utilizzo della posta elettronica, l'accesso a Internet, l'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, le modalità per effettuare i trattamenti dati;
2. il Decreto legge 9 febbraio 2012, n. 5 "Disposizioni urgenti in materia di semplificazione e di sviluppo", pubblicato nella GU 9 febbraio 2012, n. 33, all'art. 45 ha apportato semplificazioni anche in materia di dati personali, abolendo l'obbligo di adozione annuale del Documento Programmatico Sicurezza (precedentemente previsto dal Decreto legislativo

30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali);

3. permane l'obbligo di adottare le altre misure di sicurezza previste dal suddetto Decreto legislativo 196/2003, tra cui la assegnazione dei compiti e delle responsabilità alle/ai Responsabili e incaricati;
4. il Regolamento (UE) 679/2016 introduce nuovi adempimenti in materia di trattamenti di dati personali;
5. l'art.17 del D.Lgs. n. 82 del 07/03/2005 introduce l'obbligo di affidare a un unico ufficio dirigenziale la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
6. è necessario adottare, da parte dell'ufficio di cui all'art. 17 del Codice dell'amministrazione digitale, le misure di sicurezza previste per le pubbliche amministrazioni di cui alla predetta Circolare AgID N. 2/2017 entro il 31/12/2017;
7. è opportuno adottare un unico disciplinare normativo, che accorpi le disposizioni contenute nei citati "DPS" e "Disciplinare ICT e trattamenti dati" e recepisca i suddetti aggiornamenti normativi, per comunicare con estrema chiarezza alle/ai lavoratrici/lavoratori e alle/ai Responsabili le corrette modalità per l'utilizzo degli strumenti ICT aziendali loro assegnati e la modalità di effettuazione dei trattamenti dati;
8. è inoltre opportuno adottare una politica per l'ICT e i trattamenti dati, nella quale indicare le politiche di sicurezza;

Visto il decreto del Direttore generale n.192 del 30.12.2015 avente ad oggetto "Modifica del decreto del Direttore generale n. 138 del 26.09.2013 e adozione del "Disciplinare interno in materia di gestione dei rapporti tra le strutture di ARPAT ed il Collegio dei revisori";

Visto il parere positivo di regolarità contabile in esito alla corretta quantificazione ed imputazione degli effetti contabili del provvedimento sul bilancio e sul patrimonio dell'Agenzia espresso dal Responsabile del Settore Bilancio e contabilità riportato in calce;

Visto il parere positivo di conformità alle norme vigenti, espresso dal Responsabile del Settore Affari generali, riportato in calce;

Visti i pareri espressi in calce dal Direttore amministrativo e dal Direttore tecnico;

decreta

1. di approvare la nuova normativa interna sull'ICT e sui trattamenti dati, costituita dai seguenti documenti, allegati:
   - Disciplinare ICT e trattamenti dati Rev. 01 (Disciplinare sull’utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati);
   - Politica per l'ICT e i trattamenti dati Rev. 00;
2. di abrogare i seguenti decreti:
   - Decreto D.G. n. 147 del 28.4.2009 (Disciplinare ICT e trattamenti dati Rev. 00);
   - Decreto D.G. n. 149 del 31.3.2011 (Documento programmatico della sicurezza);
3. di individuare nel Settore SIRA l'articolazione organizzativa dell'Agenzia deputata allo svolgimento delle attività di cui all'art. 17 del CAD;
4. di dare mandato al Responsabile del Settore SIRA di adottare le misure minime di sicurezza previste dal CAD, per consentirne la validazione da parte del legale rappresentante di ARPAT entro il 31/12/2017.

5. di individuare quale responsabile del procedimento il Dott. Marco Chini ai sensi dell’art. 4 della L. n. 241 del 07.08.1990 e s.m.i;
6. di dichiarare il presente decreto immediatamente eseguibile, anche al fine di consentire l'attuazione delle misure minime di sicurezza di cui alla predetta circolare AgID N. 2/2017 .

Il Direttore generale
Ing. Marcello Mossa Verre*

* “Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs 82/2005. L'originale informatico è stato predisposto e conservato presso ARPAT in conformità alle regole tecniche di cui all'art. 71 del D.Lgs 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'art. 3 del D.Lgs 39/1993.”

Il Decreto è stato firmato elettronicamente da:

- Paola Querci , sostituto responsabile del settore Affari generali in data 28/12/2017
- Andrea Rossi , responsabile del settore Bilancio e Contabilità in data 28/12/2017
- Marco Chini , il proponente in data 28/12/2017
- Paola Querci , Direttore amministrativo in data 28/12/2017
- Guido Spinelli , Direttore tecnico in data 28/12/2017
- Marcello Mossa Verre , Direttore generale in data 28/12/2017

ARPAT - DIREZIONE TECNICA - Settore Sistema Informativo Regionale Ambientale

Via Porpora, 22 - 50144 - Firenze

28/12/2017

ALLEGATO A

Disciplinare ICT e trattamenti dati

Revisione 01

Disciplinare sull'utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati

Estensore: Ing. Mario Daddi

Proponente: Dott. Marco Chini

Approvazione: Ing. Marcello Mossa Verre

tel. 055.32061 - fax 055.3206324 - p.iva 04686190481 - www.arpat.toscana.it
per comunicazioni ufficiali PEC: arpat.protocollo@postacert.toscana.it - (accetta solo PEC),
per informazioni ambientali: urp@arpat.toscana.it

Indice generale

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Articolo 1
Finalità e ambito di applicazione

Il Titolare, con l'approvazione del presente Disciplinare, mette in atto le misure tecniche e organizzative per garantire, ed essere in grado di dimostrare, che il trattamento dei dati è effettuato in modo conforme alla normativa vigente.

Il presente documento disciplina l'utilizzo, la gestione, la pianificazione e il controllo delle attività che riguardano le tecnologie dell'informazione e della comunicazione (ICT) e i trattamenti dati effettuati dal personale dipendente dell'Agenzia e da tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture di ARPAT.

Il Disciplinare viene redatto per le seguenti principali finalità:

1. adottare un unico riferimento normativo per comunicare con estrema chiarezza ai lavoratori e ai Responsabili:
    - le corrette modalità per l'utilizzo degli strumenti ICT aziendali loro assegnati;
    - la modalità di effettuazione dei trattamenti dati.
2. attuare le principali disposizioni previste dalla legislazione vigente in materia di tecnologie dell'informazione e della comunicazione e privacy e, in particolare:
    - attuare gli adempimenti previsti dal D. Lgs. 196/2003 relativi alla adozione delle misure minime di sicurezza (articoli 33, 34, 35); alla definizione delle finalità e modalità dei trattamenti, ivi compreso il profilo della sicurezza (art. 28);
    - attuare gli adempimenti previsti dal Regolamento (UE) 679/2016 relativi alla protezione dei dati, tra cui adempimenti del Titolare (art. 24.), protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25), definizione dei compiti dei Responsabili dei trattamenti (art. 28), tenuta del registro delle attività di trattamento (art. 30), adozione di misure di sicurezza adeguate al rischio (art. 32), notifiche delle violazioni di dati personali all'autorità di controllo e agli interessati (articoli 33 e 34), valutazione d'impatto sulla protezione dei dati e consultazione preventiva (articoli 35 e 36);
    - attuare, nei casi in cui non vengono trattati dati personali, misure di sicurezza corrispondenti a quelle previste dal D. Lgs. 196/2003 e dal Regolamento (UE) 679/2016, al fine di garantire adeguato livello di tutela dei dati e delle informazioni trattate e unicità di gestione;
    - adempiere a quanto prescritto dal Garante per la Protezione dei dati personali nel provvedimento a carattere generale del 01/03/2007 in materia di posta elettronica e accesso a Internet, attraverso la definizione di regole comuni per tutelare i reciproci diritti e doveri di lavoratori e datore di lavoro, la sicurezza dei dati e la privacy;

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- ridurre la probabilità che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla riservatezza, integrità e disponibilità dei dati;
- rafforzare il ruolo dei servizi di posta elettronica, del sito web e della intranet dell'Agenzia, quali strumenti di comunicazione aziendale di uso generale su cui basare il conseguimento degli obiettivi di efficienza, efficacia, economicità, semplificazione;
- rafforzare e favorire l'impiego di tecnologie e software *open source*;
- rafforzare e favorire il riuso, l'accesso e la fruibilità dei dati e documenti di cui è titolare ARPAT;

3. definire il diritto dell'Amministrazione di verificare che le risorse ICT vengano utilizzate correttamente, che non si verifichino usi impropri e individuare le modalità con cui l'Amministrazione esercita tale diritto di verifica;
4. definire il diritto di lavoratori (e di terzi) a una sfera di riservatezza anche nelle relazioni lavorative.

Le prescrizioni contenute si aggiungono e integrano le norme già previste dal contratto collettivo nazionale di lavoro, dalla normativa in materia di protezione dei dati personali e tecnologie ICT e dalla documentazione di sistema vigente in ARPAT.

Articolo 2
Licenza d'uso

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- Stessa Licenza. Coloro che trasformano il materiale o si basano su di esso, sono tenuti a distribuire le loro opere con la stessa licenza CC BY-NC-SA 3.0 IT del materiale originario.

Articolo 3
Definizioni e abbreviazioni

Amministratori di sistema: sono figure professionali critiche per i trattamenti dati in quanto operano in un contesto ove possono tecnicamente accedere, anche in modo fortuito, a dati personali o riservati e sono, in molti casi, concretamente “responsabili” di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione degli stessi dati. Ad essi si applicano le disposizioni di cui all'art. 10 del presente Disciplinare.

Codice privacy: Decreto legislativo 30 giugno 2003, n. 196

Codice dell'amministrazione digitale (CAD): Decreto legislativo 7 marzo 2005, n. 82, così come modificato dal Decreto legislativo 26 agosto 2016 n. 179 recante "Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"

Data Protection Officer (DPO): acronimo inglese del Responsabile della Protezione dei Dati (RPD).

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali immagine facciale o i dati dattiloscopici (art. 4 Regolamento (UE) 679/2016).

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall’analisi di un campione biologico della persona fisica in questione (art. 4 Regolamento (UE) 679/2016).

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 (art. 4 D. Lgs. 196/2003).

Dati personali: dato personale è qualunque informazione relativa a persona fisica, identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

sociale (art. 4 Regolamento (UE) 679/2016, equivalente alla definizione data nell'art. 4 D. Lgs. 196/2003).

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4 Regolamento (UE) 679/2016).

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 (art. 4 D. Lgs. 196/2003).

Datore di lavoro: il soggetto titolare del rapporto di lavoro con il lavoratore ai sensi dell'art. 2 del D.Lgs. 81/2008.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

ICT: Tecnologie dell'Informazione e della Comunicazione (Information Communication Technology). Comprende tutto ciò che riguarda i servizi informatici (quali ad esempio la posta elettronica, l'accesso a Internet, la condivisione delle risorse, ecc.), i sistemi applicativi (quali ad esempio il sistema di protocollo informatico, i sistemi gestionali, la intranet, il sito web istituzionale, ecc.), le postazioni di lavoro, la telefonia, le reti dati, le apparecchiature per le funzioni di stampa / fotocopia / scansione / fax, ecc.

Incaricati: si tratta delle persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal responsabile. Rientra in questa categoria tutto il personale dell'Agenzia e i tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture di ARPAT. La definizione di "incaricati", che è tratta dall'art. 4 del Codice Privacy, nel presente Disciplinare si intende riferita al soggetto che tratta qualunque tipologia di dato, inclusi i "dati personali" definiti nel medesimo articolo del Codice Privacy.

Lavoratori: persone che prestano il proprio lavoro alle dipendenze di un datore di lavoro, secondo la definizione di cui all'art. 2 del D. Lgs. 81/2008. Rientra in questa categoria tutto il personale dell'Agenzia e i tutti gli altri soggetti che a vario titolo prestano servizio o attività nelle strutture di ARPAT.

Politica per l'ICT e i trattamenti dati: descrive la Politica per l'ICT e i trattamenti dati di ARPAT in coerenza con la normativa di settore (Codice dell'Amministrazione digitale, Codice Privacy e altra normativa nazionale e regionale).

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo informazioni aggiuntive,

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Registro delle attività di trattamento: registro delle attività di trattamento svolte sotto la responsabilità del Titolare. Contiene le informazioni indicate nell'art. 30 del Regolamento (UE) 2016/679. Il Registro è tenuto in forma scritta e anche in formato elettronico e, su richiesta, è messo a disposizione dell'autorità di controllo. ARPAT utilizza un unico registro per tutte le attività di trattamento svolte al suo interno.

Regolamento regionale sul trattamento dei dati sensibili e giudiziari: si tratta del regolamento regionale sul trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo", di cui al Decreto n. 6/R del 12/2/2013 del Presidente della Giunta Regionale (ed eventuali successive modificazioni).

Identifica i tipi di dati sensibili e giudiziari trattati e descrive, per queste tipologie di dati, le finalità e le operazioni eseguibili.

É emesso in attuazione dell'articolo 1, comma 1, della legge regionale 3 aprile 2006 n. 13, redatto a sua volta in applicazione dell'art. 22 del Codice Privacy "Principi applicabili al trattamento di dati sensibili e giudiziari".

Referenti ICT: nell'ambito degli incaricati vengono individuate le figure professionali critiche per il funzionamento del sistema ICT di ARPAT, denominate "Referenti ICT", i quali sono preposti alla gestione del ciclo di vita di specifiche componenti tecnologiche o funzioni in qualità di titolare o di collaboratore.

Nell'ambito dei Referenti ICT vengono individuate le figure professionali critiche per i trattamenti dati, denominate "amministratori di sistema".

L'elenco dei Referenti ICT e degli amministratori di sistema è mantenuto aggiornato sulla intranet di Agenzia.

Relazione sull'ICT: si tratta di un documento soggetto ad aggiornamento annuale, che il Titolare approva prima della predisposizione del bilancio (esercizio e investimento), dei piani di attività, del piano di formazione e del piano della qualità, su proposta del Responsabile ICT.

Contiene quanto segue:

- Descrizione dei servizi erogati e SLA garantiti;
- Criticità connesse alla sicurezza ICT e misure adottabili per la loro risoluzione;
- Necessità che riguardano le infrastrutture di supporto (rete dati, energia elettrica, condizionamento, ecc.);
- Analisi della coerenza tra l'organizzazione e l'utilizzo dell'ICT (nell'ottica di promuovere iniziative di cooperazione alla revisione della organizzazione dell'Agenzia, al fine di

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa).

Responsabile del trattamento dati (di seguito anche solo Responsabile): si tratta del soggetto preposto dal Titolare al trattamento di dati personali ai sensi dell'art. 4 del Codice Privacy e al trattamento delle altre tipologie di dati.

I Responsabili dei trattamenti dati di ARPAT sono i responsabili delle partizioni organizzative previste nell'Atto di organizzazione, figure professionali che nell'ambito delle competenze loro attribuite possiedono i requisiti previsti dall'art. 29 del Codice Privacy per tale incarico, ovvero “soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza”.

L'elenco dei Responsabili dei trattamenti dati di ARPAT è mantenuto aggiornato sulla intranet di Agenzia.

Responsabile della protezione dei dati (RPD): è designato dal Titolare ai sensi dell’art. 37 del Regolamento (UE) 2016/679, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione di dati e della capacità di assolvere i compiti cui è preposto, specificati all’art. 39 del citato Regolamento:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento (UE) 2016/679, nonché da altre disposizioni dell’Unione o dello Stato italiano relative alla protezione dei dati;

b) sorvegliare l’osservanza del Regolamento (UE) 2016/679, di altre disposizioni dell’Unione o dello Stato italiano relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l’attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d’impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

d) cooperare con l’autorità di controllo;

e) fungere da punto di contatto per l’autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva nei casi che richiedono una valutazione d’impatto sulla protezione dei dati, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Può essere un dipendente del Titolare o assolvere i suoi compiti in base a un contratto di servizi.

I suoi dati di contatto sono pubblicati dal Titolare e comunicati all’autorità di controllo.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Non riceve alcuna istruzione relativa all'esercizio dei suoi compiti. Non è rimosso o penalizzato dal Titolare o dai Responsabili dei trattamenti per l'adempimento dei propri compiti. Riferisce direttamente al Titolare. E' tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione e dello Stato Italiano. Può svolgere altri compiti e funzioni purché non diano adito a un conflitto di interessi.

Responsabile ICT: è il Responsabile della partizione organizzativa di ARPAT cui è affidata l'organizzazione, l'innovazione e le tecnologie ICT, individuata in Allegato 1. E' in possesso dei requisiti previsti per tale incarico dall'art.17 del Codice dell'amministrazione digitale, dall'art. 28 del Regolamento (UE) 2016/679 e dall'art. 10 del Decreto Legislativo 12 febbraio 1993, n. 39. Ha le responsabilità che le leggi vigenti attribuiscono alla figura del responsabile dei sistemi informativi e i compiti indicati all'art. 17 del Codice dell'amministrazione digitale.

Scheda sistema: scheda che descrive il tipo di trattamento effettuato con un sistema applicativo o, più in generale, con un sistema ICT. La scheda contiene le principali informazioni che possono interessare gli utilizzatori del servizio o del software, quali ad esempio la descrizione del sistema e delle principali tipologie di dati trattati, i criteri su cui si basa l'organizzazione e la gestione del sistema cui si riferisce, le categorie di persone che possono accedere ai dati gestiti, le eventuali regole di utilizzo, informazioni sui backup e sulle eventuali criticità.

L'elenco aggiornato delle "schede sistema" in vigore è consultabile in specifica sezione della intranet, dalla quale è possibile accedere alle stesse schede.

Scheda gestione: scheda che contiene le informazioni riservate al personale addetto all'amministrazione, gestione o manutenzione di un sistema ICT.

L'elenco aggiornato delle "schede gestione" in vigore è consultabile in specifica sezione della intranet, dal quale è possibile accedere alle stesse schede.

Strumenti elettronici: elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento (la definizione è tratta dall'art. 4 del Codice Privacy). Dunque rientrano in questa categoria i personal computer, i notebook, i tablet, i cellulari, gli smartphone, ecc.

TIC: Tecnologie dell'informazione e della comunicazione (sigla italiana corrispondente al più noto acronimo inglese ICT, Information Communication Technology).

Titolare del trattamento dati dell'Agenzia: è ARPAT, rappresentato dal Direttore Generale. Si tratta della figura professionale definita dall'art. 4 Regolamento (UE) 679/2016 e dall'art. 4 del Codice Privacy cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Trattamento dati: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

La definizione include sia i trattamenti di dati personali, sia le altre tipologie di dati.

Valutazione d'impatto sulla protezione dei dati: valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, ai sensi dell'art. 35 del Regolamento (UE) 2016/679.

E' effettuata dal Titolare, prima di procedere al trattamento, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

La valutazione è richiesta in particolare nei seguenti casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

c) il trattamento, su larga scala, di dati personali relativi a condanne penali e reati, di cui all'articolo 10 del Regolamento (UE) 2016/679;

d) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;

e) specifiche tipologie di trattamento appositamente individuate e rese pubbliche dall'autorità di controllo.

Per l'effettuazione della valutazione il Titolare si consulta con il Responsabile della protezione dei dati ed è supportato dal Responsabile ICT.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Articolo 4
Principali riferimenti normativi

I principi applicati nella stesura del presente Disciplinare sono tratti dal quadro normativo che segue:

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

1. Costituzione: articoli 15 (libertà e segretezza della corrispondenza), 97 (organizzazione dei pubblici uffici).
2. Codice civile: articoli 2087 (tutela delle conduzioni di lavoro), 2104 (diligenza del prestatore di lavoro), 2105 (obbligo di fedeltà) e 2106 (sanzioni disciplinari).
3. Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
4. Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003, noto come Codice Privacy).
5. Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005 n. 82), così come modificato dal Decreto legislativo 26 agosto 2016 n. 179 recante "Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"
6. Decreto Legislativo 12 febbraio 1993, n. 39 (Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche).
7. Decreto Legislativo 27 gennaio 2010, n. 32 (Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea – INSPIRE).
8. D.Lgs. 9 aprile 2008, n. 81 (norme in materia di tutela della salute e della sicurezza nei luoghi di lavoro, con particolare riferimento alle disposizioni sulle attrezzature munite di videoterminali): 173, 174, allegato XXXIV.
9. L. 20 maggio 1970, n. 300 (Statuto dei lavoratori): 4 (impianti audiovisivi), 7 (sanzioni disciplinari), 8 (divieto di indagini sulle opinioni), 14 (diritto di attività sindacale).
10. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR 445/2000): articoli 14 (trasmissione del documento informatico), 17 (segretezza della corrispondenza telematica).
11. Codice di comportamento dei dipendenti pubblici (DPR 62/2013).
12. Legge 7 agosto 1990 n. 241 (aggiornata con le modifiche introdotte dalla l. 15/2005 e dalla l. 80/2005) Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
13. Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni (Legge 7 giugno 2000, n. 150).

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

14. Direttiva 27.11.2003 sull'impiego della posta elettronica nelle pubbliche amministrazioni della Presidenza del Consiglio dei Ministri – Dipartimento per l'innovazione e le tecnologie.
15. “Linee guida del Garante per posta elettronica e internet”, emanate con deliberazione 1 marzo 2007 n. 13.
16. Provvedimento del 27.11.2008 del Garante per la protezione dei dati personali “Semplificazione delle misure minime di sicurezza contenute nel disciplinare tecnico, di cui all'allegato B al codice in materia di protezione dei dati personali”.
17. Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio del 15.03.06 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.
18. Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico (anno 2014), allegato alla Determinazione Commissariale n. 95/2014 del 26-06-2014 dell'Agenzia per l'Italia Digitale.
19. Legge Regionale n. 54 del 5 ottobre 2009 (Istituzione del sistema informativo e del sistema statistico regionale. Misure per il coordinamento delle infrastrutture e dei servizi per lo sviluppo della società dell’informazione e della conoscenza).
20. Legge Regionale n. 30 del 22 giugno 2009 (Nuova disciplina dell'Agenzia regionale per la protezione ambientale della Toscana (ARPAT).
21. Vigente Atto di disciplina dell'organizzazione interna di ARPAT (abbreviato in “Atto di organizzazione”).
22. Vigente Regolamento in materia di procedimento amministrativo e per l’esercizio del diritto di accesso ai documenti amministrativi ed alle informazioni ambientali.
23. Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015: “Misure minime di sicurezza ICT per le pubbliche amministrazioni”.
24. “Disciplinare per l’utilizzo della posta elettronica e di internet per l’articolazione organizzativa della Giunta regionale”, di Regione Toscana, utilizzato come riferimento per alcuni articoli.
25. Circolare AGID 18 aprile 2017 n. 2/2017

Articolo 5
Principi generali su cui si basa l'utilizzo delle risorse ICT e il trattamento dei dati aziendali

L’utilizzo delle risorse ICT messe a disposizione del personale si ispira ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell’ambito del rapporto di lavoro, in qualsiasi forma esso sia.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Le risorse ICT fornite da ARPAT si utilizzano unicamente per perseguire gli scopi lavorativi.

La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali e non.

ARPAT inoltre, deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori, anche per conseguire gli obiettivi di efficienza, efficacia ed economicità.

I trattamenti dati si ispirano ai principi che regolano la trasparenza, l'accountabiliy, la partecipazione e l'efficacia dell'azione amministrativa e che disciplinano le attività di informazione e di comunicazione delle pubbliche amministrazioni.

La gestione del livello di riservatezza dei dati, documenti e informazioni è finalizzata da una parte ad assicurare un adeguato livello di protezione dei dati personali e di altri dati riservati (quali ad esempio informazioni che riguardano l'attività amministrativa e sanzionatoria), dall'altra a promuovere la diffusione di informazioni di interesse pubblico e risponde ai criteri definiti nella "Politica per l'ICT e i trattamenti dati".

I trattamenti di dati personali rispondono ai principi della normativa sulla privacy, di seguito riassunti:

1. **liceità, correttezza e trasparenza**: sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità**: sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, effettuato in modo conforme al Regolamento (UE) 679/2016, non è considerato incompatibile con le finalità iniziali;
3. **minimizzazione dei dati**: sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esattezza**: sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
5. **limitazione della conservazione**: sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate, richieste dal Regolamento (UE) 679/2016 a tutela dei diritti e delle libertà dell'interessato;
6. **integrità e riservatezza**: sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Articolo 6
Titolarità degli strumenti, delle apparecchiature informatiche e dei dati

ARPAT è proprietaria degli strumenti e delle apparecchiature ICT assegnate ai dipendenti, ai collaboratori e a tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto o nelle strutture di ARPAT. Tali strumenti sono affidati ai medesimi con l'obbligo di custodirli con cura, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.

Gli strumenti e le apparecchiature ICT sono restituite ad ARPAT alla cessazione dell'esigenza per la quale erano state previste, ad esempio alla cessazione dell'incarico, del rapporto di lavoro, del rapporto di collaborazione, del rapporto contrattuale con ARPAT o a seguito di trasferimento presso altra struttura di ARPAT.

ARPAT è titolare dei dati che vengono prodotti dai propri dipendenti, collaboratori e da tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Agenzia.

Articolo 7
Il software

ARPAT privilegia l'open source.

Il software sviluppato dal personale di ARPAT e da tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto o nelle strutture di ARPAT è open source, distribuibile gratuitamente a terzi, con licenza GPL.

Articolo 8
Rispetto della proprietà intellettuale e delle licenze

Tutti gli incaricati sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale e non possono, sulle apparecchiature fornite, installare hardware o software né duplicare o utilizzare software che non sia stato preinstallato, installato, fornito o comunque autorizzato da ARPAT.

Articolo 9
Utilizzo dei dati

I dati e le informazioni sono beni di ARPAT.

I dati e le informazioni detenute su apparecchiature di ARPAT o altri supporti sono utilizzati dal personale, anche fuori dagli uffici di ARPAT, ai soli fini lavorativi.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Nessun dato di ARPAT o personale può essere trattato o memorizzato su dispositivi elettronici di qualsiasi tipologia, non finalizzati all'attività lavorativa.

ARPAT favorisce il riuso, l'accesso e la fruibilità dei dati e documenti di cui è titolare. Tali attività avvengono in modo controllato per assicurare il rispetto della normativa in materia di protezione dei dati personali e la riservatezza delle istruttorie.

I dati e i documenti che ARPAT pubblica, con qualsiasi modalità, senza l'espressa adozione di una licenza di uso, si intendono rilasciati come dati di tipo aperto ai sensi dell'art. 68, comma 3 del Codice dell'amministrazione digitale.

I dati e le informazioni memorizzate, elaborate e/o comunicate attraverso le apparecchiature informatiche in uso presso ARPAT possono essere oggetto di controllo da parte dell'Amministrazione per esigenze legate a motivi di sicurezza o controllo di spesa o efficienza e manutenzione dei servizi.

Articolo 10
Compiti e responsabilità

Il Titolare dei trattamenti dati con l'approvazione del presente Disciplinare designa i Responsabili di cui all'art. 4 del Codice Privacy (e all'art. 4 Regolamento (UE) 679/2016), definisce le modalità per effettuare i trattamenti dati (personali e non personali) e per assegnare i compiti agli incaricati.

I Responsabili sono identificati nei responsabili delle partizioni organizzative di ARPAT.

Hanno le responsabilità e i compiti loro attribuiti dal regolamento organizzativo di ARPAT e, inoltre, espletano i compiti assegnati nel seguito del presente articolo.

Compiti del Responsabile ICT

E' il Responsabile della partizione organizzativa cui è affidata l'organizzazione, l'innovazione e le tecnologie ICT, con i compiti indicati all'art. 17 del Codice dell'amministrazione digitale.

Coordina le attività che riguardano l'ICT e supporta il Titolare, i Responsabili e gli incaricati nella attuazione delle misure di sicurezza previste dalle disposizioni contenute nel Codice dell'Amministrazione Digitale, Codice Privacy, e altra normativa di settore.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità sui diritti e le libertà delle persone fisiche, sulla riservatezza, integrità e disponibilità dei dati, sulla continuità operativa, propone la messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

A tal fine:

1. Predispone e tiene aggiornati il Disciplinare ICT e trattamenti dati e la Politica per l'ICT e i trattamenti dati in accordo con le disposizioni contenute nella normativa di settore.
2. Predispone annualmente la Relazione sull'ICT per l'approvazione del Titolare prima della definizione dei piani annuali.
3. Predispone e tiene aggiornato il Registro dei trattamenti dati di ARPAT per l'approvazione del Titolare.
4. Predispone, tiene aggiornato e pubblica sulla intranet un elenco dei servizi erogati con informazioni sulla struttura di riferimento per l'utilizzo, sulla struttura responsabile del sistema, sui livelli di servizio garantiti, sui Referenti ICT e amministratori di sistema preposti.
5. Garantisce la disponibilità e la corretta attuazione di procedure aggiornate per il backup, la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi.
6. Effettua la nomina individuale degli amministratori di sistema stabilendo per ciascuno di essi l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, su un documento interno che mantiene aggiornato, consultabile sulla intranet e disponibile in caso di accertamenti, anche da parte del Garante.
7. Coordina le attività e verifica con cadenza almeno annuale l'operato degli amministratori di sistema.
8. Predispone e aggiorna le procedure relative alla gestione delle tecnologie dell'informazione e della comunicazione.
9. Assicura, nello svolgimento delle sue attività, che la protezione dei dati personali avvenga fin dalla progettazione e per impostazione predefinita.
10. Predispone sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di amministratori di sistema (salvo i sistemi che effettuano trattamenti per fini esclusivamente amministrativo-contabili). Le registrazioni (access log) hanno caratteristiche di

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.

11. Supporta il Titolare nella valutazione d'impatto dei trattamenti sulla protezione dei dati.
12. In caso di violazione di dati personali informa il Titolare senza ingiustificato ritardo dopo esserne venuto a conoscenza. Documenta e registra le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Supporta il Titolare nella notifica della violazione all'autorità di controllo (da fare entro 72 ore nei casi in cui la violazione presenti un rischio per i diritti e le libertà delle persone fisiche).

Compiti del Titolare

Assicura la adozione di misure di sicurezza adeguate al rischio. A tal fine:

1. Designa il Responsabile ICT.
2. Approva la Politica per l'ICT e i trattamenti dati.
3. Approva il Disciplinare ICT e trattamenti dati.
4. Approva il Registro delle attività di trattamento.
5. Designa il Responsabile della protezione dei dati, pubblica i suoi dati di contatto e li comunica all'autorità di controllo.
6. Assicura che i compiti assegnati ai Responsabili siano disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.
7. Approva la Relazione sull'ICT prima dell'approvazione dei piani annuali.
8. Approva le procedure relative alla gestione delle tecnologie dell'informazione e della comunicazione.
9. Assicura che la protezione dei dati personali avvenga fin dalla progettazione e per impostazione predefinita.
10. Effettua, ove prevista, la valutazione d'impatto sulla protezione dei dati, supportato dal Responsabile ICT, previa consultazione con il Responsabile della protezione dei dati. Consulta l'autorità di controllo qualora la valutazione indichi che il trattamento presenterebbe un rischio elevato in assenza di misure tese ad attenuare il rischio.
11. Registra qualsiasi violazione di dati personali. Documenta le circostanze a esse relative, le loro conseguenze e i provvedimenti adottati per porvi rimedio. Valuta se dalla violazione derivino rischi per i diritti e le libertà degli interessati. In caso affermativo:

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza (qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo);
- comunica la violazione agli interessati senza ingiustificato ritardo.

Compiti assegnati al Responsabile della protezione dei dati

1. Informa e fornisce consulenza al Titolare, ai Responsabili e agli incaricati in merito agli obblighi derivanti dal Regolamento (UE) 679/2016, dal Codice Privacy e da altre disposizioni normative relative alla protezione dei dati.
2. Sorveglia l'osservanza del Regolamento (UE) 679/2016, del Codice Privacy e di altre disposizioni normative relative alla protezione dei dati, nonché delle politiche del Titolare in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle attività di controllo.
3. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento.

Compiti assegnati a tutti i Responsabili

1. Espletano i compiti istituzionali della partizione organizzativa che coordinano, nel rispetto delle:
   - disposizioni generali, valide per tutti i trattamenti dati, contenute nel presente Disciplinare, nella Politica per l'ICT e i trattamenti dati e successive disposizioni applicative;
   - ulteriori disposizioni del Codice Privacy e Regolamento (UE) 679/2016, che si applicano alle specifiche attività istituzionali della struttura che coordinano.
2. Definiscono l'ambito di trattamento consentito ai singoli incaricati tramite:
   - assegnazione formale delle attività e degli obiettivi;
   - definizione dei profili di autorizzazione del personale interno ed esterno che svolge attività per conto della struttura che coordinano. A tal fine:
     i. effettuano le richieste di accesso alle applicazioni mediante apposita modulistica;
     ii. verificano periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione del personale interno ed esterno che svolge attività per conto della struttura che coordinano;
     iii. assicurano che l'ambito di trattamento assegnato ai singoli incaricati sia coerente ai compiti loro assegnati tenendo anche conto dei principi di adeguatezza, proporzionalità e necessità.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

3. Garantiscono che le persone autorizzate al trattamento dei dati personali e dei dati riservati si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
4. Vigilano sul rispetto delle disposizioni contenute nel presente Disciplinare e collaborano alla attuazione delle misure indicate.
5. Non ricorrono ad altri Responsabili del trattamento senza l'autorizzazione scritta del Titolare.
6. Tenendo conto della natura del trattamento, assistono il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti degli interessati di cui al capo III del Regolamento (UE) 2016/679 (art. 12 e successivi).
7. Assistono il Titolare nel garantire gli obblighi di cui agli articoli da 32 a 36 del Regolamento (UE) 2016/679:
    - adozione di adeguate misure sicurezza;
    - cooperazione con l'autorità di controllo;
    - notifica di violazione dei dati personali (in caso di violazione di dati personali informano il Titolare senza ingiustificato ritardo dopo esserne venuti a conoscenza. Documentano e registrano le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio);
    - comunicazione delle violazioni agli interessati;
    - valutazione d'impatto sulla protezione dei dati e consultazione preventiva.
8. Su scelta del Titolare, cancellano o restituiscono agli interessati tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellano le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri ne preveda la conservazione.
9. Mettono a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei loro obblighi e contribuiscono alle attività di revisione, comprese le ispezioni, realizzati dal Titolare (o da altro soggetto da questi incaricato).
10. Informano immediatamente il Titolare qualora ritengano che un'istruzione violi la normativa sulla privacy.
11. **In caso di trattamento di dati riservati**:
    i. definiscono i settori di lavorazione o i singoli incaricati che possono trattare queste tipologie di dati e assicurano che siano adottate le specifiche misure minime di sicurezza previste in questi casi (vedi Allegato 2);
    ii. prescrivono adeguate misure di sicurezza aggiuntive qualora ritengano che le misure minime prescritte nel Disciplinare non siano idonee a trattare la tipologia dei dati

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

personali e delle informazioni gestite dalla propria struttura, definendo tali misure in apposita Scheda sistema o gestione;

iii. assicurano che il trattamento dei dati sensibili e giudiziari sia conforme a quanto prescritto dall'apposito Regolamento regionale sul trattamento dei dati sensibili e giudiziari.

12. Individuano e nominano, ove necessario, le figure professionali critiche per il funzionamento del sistema ICT (Referenti ICT) e per i trattamenti dati (amministratori di sistema) e comunicano tali nomine al Responsabile ICT.
13. Assicurano la formazione di base dei propri collaboratori interni ed esterni in materia di sicurezza informatica e privacy (la formazione è effettuata al momento dell'ingresso dei collaboratori presso la struttura, nonché in occasione dei cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati).
14. Assicurano la presenza di procedure e regole di utilizzo per la gestione di eventuali strumenti informatici dei quali hanno il completo controllo diretto o la gestione applicativa, mediante elaborazione Scheda sistema e/o gestione.
15. Partecipano al processo di pianificazione delle attività ICT segnalando le necessità informatiche della struttura che coordinano.

Compiti aggiuntivi assegnati ai Responsabili

Ad alcuni Responsabili, individuati in Allegato 1, sono assegnati specifici compiti aggiuntivi necessari ad assicurare adeguato livello di tutela dei dati e delle informazioni trattate in ARPAT. Tali compiti sono mirati principalmente ad assicurare:

- la continuità di funzionamento delle infrastrutture di supporto (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- la protezione delle aree e dei locali;
- la sicurezza nella gestione operativa dei beni ICT;
- la protezione degli apparati critici (server, router, ecc.);
- la protezione dei cablaggi critici (dorsali della rete dati, cavi di alimentazione degli apparati critici);
- lo svolgimento di alcune attività critiche relative alla gestione delle risorse umane (note informative ai nuovi incaricati; note informative su assunzioni, cessazioni, trasferimenti, nomine Responsabili; formazione in materia di sicurezza informatica e privacy e rendicontazione).

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Compiti assegnati agli incaricati

Gli incaricati svolgono le attività loro assegnate nel rispetto delle misure minime di sicurezza riportate in Allegato 2.

Compiti dei Referenti ICT

Nell'ambito degli incaricati sono individuati i Referenti ICT, figure professionali critiche per il funzionamento dei sistemi ICT.

I Referenti ICT curano la gestione del ciclo di vita di specifiche componenti tecnologiche o funzioni in qualità di titolare o di collaboratore (gestione, controllo della configurazione e documentazione dei sistemi/funzioni a cui sono assegnati).

Disposizioni relative ad amministratori di sistema

Nell'ambito dei Referenti ICT sono individuati gli amministratori di sistema, figure professionali critiche per il funzionamento dei sistemi ICT e per i trattamenti dati, per i quali valgono le disposizioni aggiuntive riportate nel seguito.

Con la definizione di “amministratore di sistema” si individuano sia le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (che è la definizione che viene comunemente data in ambito informatico di amministratore di sistema), sia gli amministratori di database, gli amministratori di rete, gli amministratori di apparati di sicurezza, gli amministratori di sistemi software complessi.

Gli amministratori di sistema sono figure professionali critiche per i trattamenti dati in quanto:

- operano in un contesto ove possono tecnicamente accedere, anche in modo fortuito, a dati personali o riservati sebbene non siano preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni);
- sono, in molti casi, concretamente “responsabili” di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione degli stessi dati.

L'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.

Anche nei casi in cui le funzioni di amministratore di sistema sono attribuite solo nel quadro di una designazione quale “incaricato” del trattamento, il Titolare e il Responsabile devono comunque attenersi a criteri di valutazione equipollenti a quelli richiesti per la designazione dei “Responsabili”.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

La rilevanza, la specificità e la particolare criticità del ruolo di amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter) nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (articoli 635 quater e quinques).

La designazione quale amministratore di sistema è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'attribuzione di funzioni di amministratore di sistema avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti designati, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Articolo 11
Modalità per effettuare i trattamenti dati

Trattamenti dati effettuati in Agenzia e strumenti utilizzati

In Agenzia sono effettuati e consentiti i soli trattamenti dati che riguardano l'espletamento dei compiti istituzionali di ARPAT, i quali sono esplicitati, per ciascuna struttura, nell'Atto di organizzazione.

Per i trattamenti di dati personali sensibili e giudiziari si applicano inoltre le ulteriori disposizioni regionali contenute nel regolamento regionale sul trattamento dei dati sensibili e giudiziari.

Per tutti i trattamenti sono utilizzati personal computer connessi in rete e strumenti di office automation.

Alcuni trattamenti sono effettuati con specifici sistemi ICT (ad esempio posta elettronica, condivisione delle risorse, intranet, sito istituzionale, sistema di protocollo informatico e gestione documentale, ecc.), che sono descritti in appositi moduli, denominati “schede sistema” e “schede gestione”.

I principali elementi che costituiscono il sistema ICT di ARPAT sono descritti, nel loro insieme, nella Relazione sull'ICT e, in dettaglio, nelle Schede sistema e gestione, dei singoli applicativi e componenti tecnologiche, a cui si rimanda per ulteriori dettagli e specificità.

Le schede sistema sono destinate agli utilizzatori. Contengono per ciascun sistema le seguenti informazioni:

- una descrizione del sistema ICT e del trattamento effettuato (tipologie di dati trattati, principali caratteristiche del sistema, informazioni sui backup e sulle eventuali criticità);

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- i criteri su cui si basa l'organizzazione, la gestione del sistema e l'accesso ai dati trattati;
- le registrazioni informatiche, ovvero i dati e i documenti prodotti dall'applicativo di cui è prevista la conservazione per legge o regolamento e i tempi di conservazione previsti;
- le eventuali regole di utilizzo.

Le schede gestione sono destinate ai tecnici manutentori, denominati “Referenti ICT”. Contengono, per ciascun sistema, le informazioni necessarie ad assicurare interscambiabilità e continuità operativa, quali:

- le procedure di intervento che devono essere eseguite in caso di emergenza e tutte le informazioni che consentano a un tecnico informatico (e in alcuni casi anche a un non informatico) che non conosce la configurazione del sistema specifico, di ripristinarne il funzionamento in caso di guasto;
- le informazioni necessarie a reperire rapidamente la documentazione applicabile e il software eventualmente occorrente a eseguire le procedure di intervento nei casi di emergenza;
- la descrizione delle attività che riguardano la amministrazione/gestione del sistema.

Le schede sistema e gestione sono poste sulla intranet per consultazione, insieme al loro elenco, avendo cura di proteggere le informazioni riservate da accessi non autorizzati.

Strutture di riferimento, strutture che concorrono al trattamento dei dati

Le strutture di riferimento per tutte le tipologie di trattamenti sono le partizioni organizzative dell'Agenzia e ciascuna di esse concorre al trattamento secondo le competenze definite nell'Atto di organizzazione. Il relativo responsabile è, ai sensi dell’art. 4 del Regolamento (UE) 679/2016 e dell’art. 4 del Codice Privacy, il responsabile dei trattamenti dati nella struttura che coordina.

L'elenco aggiornato delle strutture di riferimento e dei relativi Responsabili ai fini dei trattamenti dati viene mantenuto aggiornato sulla intranet.

Trattamenti in outsourcing

I Responsabili che si avvalgono di soggetti esterni all’Agenzia assicurano:

1. che il trattamento sia autorizzato preventivamente in forma scritta dal Titolare (come da art. 28 comma 2 del Regolamento (UE) 679/2016);
2. che il trattamento sia conforme alle disposizioni contenute nel D.Lgs. 196/2003 e nel Regolamento (UE) 679/2016 mediante adozione di misure di sicurezza adeguate alla tipologia e riservatezza dei dati trattati quali, ad esempio, clausole contrattuali che prevedano:

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

a) obblighi di comunicazione, da parte del soggetto esterno, degli estremi identificativi del Responsabile del trattamento da questi effettuato;

b) l'attestazione di conformità del trattamento alle disposizioni contenute nel D.Lgs. 196/2003, nel Regolamento (UE) 679/2016 e alle disposizioni di legge relative alla sicurezza dei sistemi informativi delle pubbliche amministrazioni (esempio misure minime di sicurezza) da parte del soggetto esterno;

c) l'accettazione, da parte del soggetto esterno, delle regole stabilite nel presente Disciplinare, qualora il trattamento sia effettuato con strumenti ICT di ARPAT;

d) obblighi di comunicazione, da parte del soggetto esterno, degli estremi identificativi delle persone fisiche che svolgono le funzioni di amministratore di sistema, con la descrizione delle funzioni ad esse attribuite;

e) la consegna, con periodicità adeguata alla tipologia di servizio fornito, dei dati significativi di backup da parte del soggetto esterno, ovvero dei dati necessari a poter migrare in autonomia ad altro fornitore;

f) la riservatezza professionale di tutto il personale del soggetto esterno designato alla esecuzione del contratto (non rivelare informazioni o dati venuti a conoscenza nel corso dell'esecuzione del contratto mantenendole segrete);

g) il rispetto delle basilari norme di comportamento in materia di sicurezza informatica da parte di tutto il personale del soggetto esterno designato alla esecuzione del contratto, quali ad esempio: non condividere le credenziali assegnate con altri utenti (qualora ciò accada, anche per motivi fortuiti, richiedere il reset della password al supporto sistemistico di ARPAT); custodire diligentemente le credenziali assegnate; non lasciare incustodito e accessibile il dispositivo elettronico durante una sessione di collegamento alla rete di Arpat, bensì bloccare il computer; non divulgare, comunicare, cedere a terzi informazioni relative all'infrastruttura di Arpat; non svolgere attività che possano facilitare l'accesso ad essa da parte di personale non autorizzato, non manomettere la configurazione dei sistemi; attenersi alle istruzioni ricevute per l'accesso ai servizi; non tentare di accedere a servizi non consentiti, non tentare di acquisire privilegi di superuser o administrator;

h) poteri di verifica, da parte di ARPAT, in merito alle modalità operative adottate per il trattamento da parte del soggetto esterno;

i) applicazione di penali proporzionate alla gravità della mancanza qualora il trattamento effettuato non risulti conforme alle disposizioni contenute nel presente Disciplinare;

2. la conservazione, per ogni eventuale evenienza, della documentazione ricevuta dal soggetto esterno di cui al precedente punto 1;

3. la verifica dell'operato del soggetto esterno;

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

4. l'attuazione delle misure necessarie a consentire la migrazione ad altro fornitore qualora l'oggetto del trattamento riguardi dati e informazioni strategiche per il funzionamento di ARPAT.

Formazione degli incaricati

La formazione di base è assicurata mediante:

- comunicazione metodica ai nuovi assunti delle istruzioni relative all'utilizzo dei sistemi ICT, alle modalità per i trattamenti dati e diffusione di queste istruzioni sulla intranet;
- capillare diffusione del presente Disciplinare;
- pubblicazione, sulla intranet, delle schede sistema descrittive dei singoli sistemi ICT in uso in Agenzia, che costituiscono la guida di riferimento per gli utenti;
- rilevazione dei bisogni formativi mediante periodici sondaggi;
- pubblicazione, sulla intranet, di corsi in materia di sicurezza informatica e privacy.

La formazione è effettuata al momento dell'ingresso del personale presso la struttura, nonché in occasione dei cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati.

Inoltre, sono programmati specifici interventi formativi con obbligo di partecipazione da parte del personale designato.

Articolo 12
Utilizzo della Posta elettronica

Il servizio di posta elettronica erogato dai sistemi di ARPAT è ad uso esclusivo di ARPAT.

Ogni comunicazione via posta elettronica con soggetti esterni o interni all'amministrazione deve avvenire esclusivamente mediante l'utilizzo del sistema di posta elettronica di ARPAT, per garantire i necessari livelli di sicurezza e riservatezza.

A tal fine ARPAT assegna una casella di posta personale a tutto il personale che ha un rapporto di lavoro con l'Agenzia e che risulti abile all'utilizzo del servizio. Gli assegnatari delle caselle di posta sono tenuti a consultarle, a gestirle e a ripulirle periodicamente dallo spam.

I messaggi trasmessi si intendono inviati e pervenuti ai destinatari se trasmessi agli indirizzi di posta loro assegnati (nel caso si tratti di personale interno e quindi di caselle del dominio ARPAT) o dichiarati (nel caso si tratti di soggetti esterni). Quanto alla certezza della ricezione del messaggio da parte del destinatario, il mittente, ove ritenuto necessario, può richiedere al destinatario stesso un messaggio di risposta che confermi l'avvenuta ricezione.

L'assegnazione delle caselle di posta elettronica ai dipendenti è finalizzata all'utilizzo di tale mezzo di comunicazione per lo svolgimento dell'attività lavorativa. Ad esempio non è consentito utilizzare l'indirizzo di posta elettronica aziendale per:

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- motivi non attinenti allo svolgimento delle mansioni assegnate;
- la partecipazione a dibattiti, forum o mailing list su Internet per motivi non professionali;
- aderire o rispondere a messaggi che invitano a perpetuare verso ulteriori indirizzi di posta elettronica contenuti o documenti oggetto delle cosiddette “catene di S. Antonio”;
- effettuare ogni genere di comunicazione finanziaria ivi comprese le operazioni “remote banking”, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione aziendale.

Inoltre, non è consentito:

- simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta non proprie per l'invio di messaggi;
- prendere visione della posta altrui;
- aprire messaggi di posta ambigui e di incerta provenienza (gli allegati possono infatti contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati);
- l'invio a mezzo posta elettronica di dati sensibili, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati personali;
- divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui.

Articolo 13
Utilizzo di Internet

Il collegamento a Internet, reso disponibile sulle postazioni di lavoro, è finalizzato all’utilizzo di tale mezzo di comunicazione per lo svolgimento dell’attività lavorativa. Ad esempio non è consentito:

- navigare in siti Internet non attinenti allo svolgimento delle mansioni assegnate;
- effettuare ogni genere di transazione finanziaria ivi comprese le operazioni “remote banking”, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione aziendale;
- lo scarico di software prelevati dai siti Internet, salvo diversa ed esplicita autorizzazione aziendale;
- ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- la partecipazione, per motivi non professionali, a forum, chat line, bacheche elettroniche, registrazioni in guest book, anche utilizzando pseudonimi (nickname);
- scaricare materiale di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Articolo 14
Utilizzo della intranet e del sito web

La intranet e il sito web sono i principali strumenti utilizzati per pubblicare o condividere in sicurezza contenuti in rete (quali informazioni, notizie, documenti, comunicazioni, decreti, procedure, manuali, ecc.) che riguardano i trattamenti dati effettuati da ARPAT.

Si utilizza la intranet per la pubblicazione o condivisione di contenuti che interessano tutto il personale dell'Agenzia o specifiche categorie di utenti interni.

Si utilizza il sito web per la pubblicazione di contenuti che interessano i cittadini o specifiche categorie di soggetti esterni all'Agenzia.

Tramite la intranet e il sito web è inoltre possibile accedere ai principali applicativi e servizi di rete basati su tecnologia web.

I file che vengono inseriti nella intranet e nel sito web devono essere prodotti preferibilmente con strumenti open source.

Articolo 15
Tipologia delle informazioni memorizzate relative all'utilizzo delle risorse ICT, finalità e modalità di gestione

a) Informazioni memorizzate relative a telefonia di rete fissa, telefonia mobile, telefonia via Internet, posta elettronica, accesso a Internet

Sono memorizzate da parte di ARPAT le seguenti informazioni ove ciò sia possibile:

1. i dati necessari per rintracciare e identificare la fonte di una comunicazione;
2. i dati necessari per rintracciare e identificare la destinazione di una comunicazione;
3. i dati necessari per determinare la data, l'ora e la durata di una comunicazione;
4. i dati necessari per determinare il tipo di comunicazione;
5. i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature.

b) Informazioni memorizzate relative ad altri servizi ICT

Sono memorizzate da parte di ARPAT le seguenti informazioni ove ciò sia possibile:

1. i dati necessari per determinare la data, l'ora e la durata di accesso al servizio;
2. i dati necessari per determinare il tipo di servizio utilizzato;
3. i dati necessari per identificare il tipo di operazioni effettuate;

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

4. i dati necessari per determinare le attrezzature utilizzate per accedere al servizio;
5. ulteriori dati qualora siano previsti da specifiche leggi, norme o regolamenti di settore.

Finalità delle informazioni salvate e durata della conservazione

Le informazioni di cui ai precedenti paragrafi a) e b) sono tracciate e conservate per finalità organizzative di sicurezza e di controllo da parte dell'Agenzia per i periodi minimi e massimi stabiliti dalle norme vigenti.

Articolo 16
Controlli e sanzioni

A garanzia della sicurezza dei sistemi informativi e dei servizi di rete, è nella facoltà di ARPAT effettuare controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree, nonché predisporre controlli a campione, in forma anonima, sull'utilizzo delle risorse ICT per le quali è riconosciuto il diritto del lavoratore (e dei terzi) a una sfera di riservatezza anche nelle relazioni lavorative, come ad esempio nell'uso della posta elettronica, nell'accesso a Internet/intranet, nell'uso delle condivisioni personali e servizi ad essi assimilabili.

È sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nelle seguenti necessità:

- corrispondere a eventuali richieste di organi di polizia su segnalazione dell'autorità giudiziaria;
- nel verificarsi di un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature;
- specifiche richieste dell'interessato relative a dati che lo riguardano.

A garanzia della sicurezza dei sistemi informativi, dei servizi di rete e dei dati aziendali è, tuttavia, nella facoltà di ARPAT effettuare controlli puntuali sulla applicazione delle norme contenute nel presente Disciplinare che non riguardano la sfera di riservatezza riconosciuta al lavoratore (quali ad esempio il rispetto delle norme generali di comportamento, la verifica dell'operato degli amministratori di sistema, ecc.) da parte dei Responsabili.

ARPAT non effettuerà trattamenti di dati personali mediante sistemi hardware e/o software che mirino al controllo a distanza dei lavoratori quali:

- lettura e/o registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Nei casi di accertata violazione dei principi fissati nel presente Disciplinare, è demandata ai singoli dirigenti preposti l'applicazione dei provvedimenti disciplinari individuati nel CCNL con le modalità ivi previste per il personale dipendente o equiparato, l'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Allegato 1
Compiti aggiuntivi dei Responsabili

(ai sensi dell'art. 29 del Decreto legislativo 30 giugno 2003, N. 196 e dell'art. 10 del Disciplinare ICT e trattamenti dati Rev. 01)

Ai Responsabili individuati nel presente Allegato:

- Direttore amministrativo
- Direttore tecnico
- Coordinatori di Area Vasta
- Responsabili dei dipartimenti che non sono sede di Area Vasta
- Responsabile Settore SIRA
- Responsabile Settore Affari generali
- Responsabile Settore Gestione delle risorse umane
- Responsabile Settore Patrimonio immobiliare impianti e reti
- Responsabili dei Settori Attività amministrative e Provveditorato

sono assegnati specifici compiti aggiuntivi, necessari ad assicurare adeguato livello di tutela dei dati e delle informazioni trattate, che si aggiungono a quelli già definiti all'art. 10 del Disciplinare.

Direttore amministrativo

Assicura che l'accesso in Agenzia presso la Direzione avvenga in modo controllato.

Direttore tecnico

Cura il coordinamento della predisposizione delle proposte di investimento relative alla dotazione tecnologica dell'Agenzia in coerenza con:

- Politica per l'ICT e i trattamenti dati;
- contenuti della Relazione sull'ICT.

Coordinatori di Area Vasta

Assicurano d'intesa con il Settore SIRA, presso la sede dell'Area vasta di competenza, il rispetto delle politiche di sicurezza relative alla gestione delle infrastrutture di supporto e alla protezione delle aree e dei locali, con particolare riferimento a quanto segue:

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- controllo degli accessi ai locali della sede;
- gestione operativa dei servizi di supporto necessari al corretto funzionamento dei sistemi informatici (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- gestione operativa, in collaborazione con il Settore SIRA, dei beni ICT dislocati presso la sede;
- protezione degli apparati critici (quali ad esempio i server e altri apparati critici dislocati presso la sede);
- protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari).

Assicurano, presso la Area vasta di competenza, il controllo sulla attuazione del Disciplinare ICT e trattamenti dati.

Responsabili dei dipartimenti che non sono sede di Area Vasta

Assicurano d'intesa con il Settore SIRA, presso la sede di competenza, il rispetto delle politiche di sicurezza relative alla gestione delle infrastrutture di supporto e alla protezione delle aree e dei locali, con particolare riferimento a quanto segue:

- controllo degli accessi ai locali della sede;
- gestione operativa dei servizi di supporto necessari al corretto funzionamento dei sistemi informatici (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- gestione operativa, in collaborazione con il Settore SIRA, dei beni ICT dislocati presso la sede;
- protezione degli apparati critici (quali ad esempio i server e altri apparati critici dislocati presso la sede);
- protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari).

Responsabile Settore SIRA

É il Responsabile ICT di ARPAT.

Assicura il rispetto delle politiche di sicurezza relative alla gestione operativa dei beni ICT dislocati presso la Direzione.

Responsabile Settore Affari generali

Assicura la pubblicazione sulla intranet aziendale della normativa regionale in materia di trattamenti dati personali sensibili e giudiziari.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Responsabile Settore Gestione delle risorse umane

- Tiene un aggiornato elenco delle strutture di riferimento per i trattamenti di dati personali e relativi responsabili, con pubblicazione sulla intranet.
- Rileva le necessità di formazione in materia di privacy.
- Cura le seguenti attività:
  - comunicazione ai nuovi assunti di una nota informativa, predisposta dal Settore SIRA, in materia di utilizzo dei sistemi informatici, telefonia e tutela della privacy;
  - comunicazione delle assunzioni, cessazioni, trasferimenti, nomine dei Responsabili al Settore SIRA, al Settore Provveditorato, ai Settori Amministrativi;
  - organizzazione e programmazione dei corsi in materia di sicurezza informatica e privacy previsti nel piano di formazione;
  - rendicontazione dei corsi effettuati in materia di sicurezza informatica e privacy.

Responsabile Settore Patrimonio immobiliare impianti e reti

Assicura, d'intesa con il Responsabile Settore SIRA, il rispetto delle politiche per la gestione delle infrastrutture di supporto e la protezione delle aree e dei locali relativamente a quanto segue:

- servizi di supporto al funzionamento dei sistemi informatici (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- protezione degli apparati critici (server, apparati di rete, ecc. in locali climatizzati, protetti da accessi non autorizzati, dotati di sistemi antincendio).
- protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari).

Cura la gestione operativa delle attività che riguardano le infrastrutture di supporto e la protezione delle aree e dei locali presso la sede della Direzione, relativamente agli aspetti sopra indicati.

Responsabili dei Settori Attività amministrative e Provveditorato

Assicurano, in qualità di consegnatari:

- la tenuta di un inventario aggiornato dei beni ICT di competenza, in stretto raccordo con il Settore SIRA, nonchè con gli utilizzatori dei beni informatici, che a tale proposito sono tenuti a fornire tempestivamente ogni utile informazione relativa alla gestione inventariale di tali beni;
- che i beni ICT di competenza siano restituiti ad ARPAT alla cessazione dell'esigenza per la quale erano stati previsti (ad esempio alla cessazione dell'incarico, del rapporto di

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

lavoro, del rapporto di collaborazione, del rapporto contrattuale con ARPAT o a seguito di trasferimento presso altra struttura di ARPAT).

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Allegato 2
Norme generali di comportamento prescritte agli incaricati

(ai sensi dell'Allegato B del Decreto legislativo 30 giugno 2003, N. 196 e dell'art. 10.e del Disciplinare ICT e trattamenti dati Rev. 01)

1. Disposizioni generali sull'utilizzo dei sistemi ICT e sui trattamenti dati

Ciascun incaricato effettua i trattamenti dati relativi alle funzioni cui è assegnato attenendosi a quanto segue:

1. disposizioni generali contenute nel Disciplinare;
2. norme di comportamento contenute nel presente allegato;
3. regole di utilizzo dei singoli sistemi ICT impiegati per l'espletamento delle proprie attività lavorative, contenute nelle “Schede sistema” dei sistemi utilizzati (ad esempio: posta elettronica, protocollo informatico, sito web istituzionale, intranet, ecc.);
4. principi generali e finalità su cui si basa l'utilizzo delle risorse ICT e il trattamento dei dati aziendali (definiti nell'art. 5 del Disciplinare ed esplicitati nella Politica per l'ICT e i trattamenti dati di ARPAT) di seguito richiamati:
   a) diligenza e correttezza nell’uso degli strumenti ICT;
   b) utilizzare le risorse ICT dell'Agenzia unicamente per perseguire gli scopi lavorativi;
   c) adeguata protezione dei dati e delle informazioni, in maniera da evitare trattamenti non autorizzati, illeciti, perdita o distruzione;
   d) il rispetto delle regole è necessario per assicurare il corretto funzionamento degli strumenti informatici e consentire ad ARPAT di conseguire gli obiettivi di efficienza, efficacia ed economicità;
   e) favorire la trasparenza, l’accountability, la partecipazione, l’efficacia dell’azione amministrativa;
   f) assicurare la riservatezza professionale nelle istruttorie riservate (ad esempio quelle relative alle attività amministrativa e sanzionatoria);
   g) favorire la diffusione delle informazioni di interesse pubblico attraverso i canali previsti;
   h) rispettare i principi della normativa sulla protezione dei dati personali, stabiliti per i trattamenti dati: liceità, correttezza, trasparenza, limitazione delle finalità in base alle quali si raccolgono i dati (determinate, esplicite e legittime), minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza;
5. eventuali ulteriori istruzioni del preposto Responsabile.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Ciascun incaricato è personalmente responsabile del corretto utilizzo dei sistemi ICT che gli sono stati affidati e dei dati che inserisce o modifica negli applicativi.

2. Misure minime di sicurezza prescritte per tutti gli incaricati che effettuano trattamenti dati con l'ausilio di strumenti elettronici

Ogni Incaricato che tratta dati con gli strumenti elettronici è vincolato alle seguenti norme generali di comportamento:

1. acquisire le nozioni di base sulla sicurezza informatica e la privacy consultando le informazioni iniziali per i nuovi assunti sull'utilizzo dei sistemi informatici, telefonia e tutela della privacy e frequendando i corsi cui è invitato a partecipare;
2. non condividere il proprio account con altri utenti (a meno che non sia espressamente previsto);
3. non cedere a terzi la propria password, a meno che ciò non sia espressamente previsto; qualora ciò accada, anche per motivi fortuiti, richiedere il reset della password al referente dell'applicativo;
4. utilizzare password di almeno 8 caratteri non facilmente riconducibili all'incaricato, contenenti anche numeri o caratteri speciali; nel caso in cui lo strumento elettronico non lo consenta, la password dovrà essere composta dal numero di caratteri pari al massimo consentito; per le utenze amministrative è richiesta maggiore robustezza (almeno 14 caratteri contenenti anche numeri e caratteri speciali);
5. cambiare la password al primo utilizzo e successivamente almeno ogni 3 mesi;
6. non lasciare incustodito e accessibile lo strumento elettronico durante una sessione del trattamento, bensì bloccare il computer e, inoltre, configurare il salvaschermo nella modalità di attivazione automatica;
7. non lasciare incustoditi e accessibili i dispositivi portatili;
8. salvare i dati e i documenti sui server;

   Note:

   a) per il salvataggio utilizzare gli appositi servizi di rete cui si è abilitati, quali ad esempio:

      - condivisioni di rete;
      - intranet;
      - sito web;
      - sistema di protocollo informatico e gestione documentale;
      - altri applicativi di rete.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

b) è altresì possibile salvare copie di lavoro dei dati e dei documenti non riservati sulle postazioni di lavoro e sui dispositivi mobili (notebook, smartphone, tablet, ecc.);

c) è altresì possibile salvare copie di lavoro dei dati e dei documenti riservati su supporti removibili a condizione di rispettare le misure previste per i trattamenti dei dati sensibili giudiziari o comunque riservati (vedi successivo paragrafo 4);

9. navigazione Internet: non visitare / scaricare / eseguire file da siti poco sicuri;
10. posta elettronica: non aprire alcun allegato sospetto né seguire collegamenti sospetti, dove per sospetto si intende non atteso e proveniente da mittenti sconosciuti;
11. conoscere le caratteristiche dei sistemi e servizi informatici utilizzati e attenersi alle norme di utilizzo se presenti (le quali sono contenute nelle schede sistema, pubblicate sulla intranet);
12. non eseguire o installare software senza autorizzazione da parte della struttura responsabile dell'ICT e senza verifica che tale software sia libero da virus;
13. non tentare di accedere a servizi loro non consentiti;
14. non tentare di acquisire privilegi di superuser o administrator;
15. non collegare modem o comunque dispositivi che consentano un accesso non controllato a Internet o ad apparati (router, sistemi di elaborazione, personal computer connessi in rete, ecc.) della rete privata dell'ARPAT;
16. spegnere i propri strumenti di lavoro al termine della giornata lavorativa a meno che non vi siano diverse motivate disposizioni contrarie;
17. non intercettare, alterare, impedire o interrompere comunicazioni di altri utilizzatori o servizi della Rete; non installare apparecchiature idonee a tale scopo, salvo che queste attività non siano atte a garantire le previste misure di sicurezza di ARPAT;
18. nei casi dubbi (su come comportarsi) chiedere chiarimenti e/o istruzioni scritte al competente Responsabile.

3. Misure minime di sicurezza prescritte per tutti gli incaricati che effettuano trattamenti dati senza l'ausilio di strumenti elettronici

1. Custodire e controllare, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti avuti in carico contenenti dati personali e altre tipologie di dati e assicurare che siano restituiti al termine delle operazioni affidate;
2. Assicurare che agli atti e documenti avuti in carico che contengano dati o informazioni riservate non accedano persone prive di autorizzazione;
3. Assicurare che:
   - l'accesso agli archivi contenenti dati o informazioni riservate sia controllato;

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, siano identificate e registrate;
- quando gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono siano preventivamente autorizzate.

4. nei casi dubbi (su come comportarsi) chiedere chiarimenti e/o istruzioni scritte al competente Responsabile.

4. Misure minime di sicurezza prescritte per tutti gli incaricati che trattano dati riservati

I dati riservati includono i dati personali che nel Codice Privay sono definiti sensibili e giudiziari, i dati personali che nel Regolamento (UE) 679/2016 sono definiti dati genetici, dati biometrici, dati relativi alla salute e qualunque altra tipologia di dato definito riservato dal competente Responsabile o nella scheda descrittiva del sistema (scheda sistema).

I trattamenti di dati riservati richiedono esplicita autorizzazione scritta da parte del competente Responsabile che, nel caso di dati sensibili e giudiziari, verifica che il trattamento si svolga nel rispetto del Decreto del Presidente della Giunta Regionale n. 18 del 18.5.2006 (Regolamento sul trattamento dei dati sensibili e giudiziari).

Per i trattamenti di dati riservati valgono le seguenti regole aggiuntive:

1. utilizzare sistemi applicativi abilitati al trattamento delle suddette tipologie di dati.
2. effettuare trattamenti con strumenti di Office Automation o altri strumenti di produttività personale esclusivamente se i dati risiedono:
   - in una apposita cartella ubicata su un server, ove possa accedere il solo personale abilitato secondo la procedura prevista dal servizio di condivisione delle risorse;
   - su supporti rimovibili conservati e gestiti come indicato nel seguito;
3. custodire e conservare gli eventuali supporti rimovibili utilizzati per memorizzare i dati in armadi chiusi a chiave o secondo le eventuali disposizioni scritte impartite dal competente responsabile;
4. svolgere le azioni necessarie ad assicurare che i supporti removibili non più utilizzati, che hanno contenuto dati riservati, siano distrutti o resi inutilizzabili, salvo seguire apposite disposizioni al riguardo, approvate dal Responsabile ICT;
5. nei casi dubbi (su come comportarsi) chiedere chiarimenti e/o istruzioni scritte al competente Responsabile.

tel. 055.32061 - PEC: ARPAT.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

ARPAT - DIREZIONE TECNICA - Settore Sistema Informativo Regionale Ambientale

Via Porpora, 22 - 50144 - Firenze

21/12/2017

ALLEGATO B

Politica per l'ICT e i trattamenti dati

Revisione 00

(ai sensi dell'art. 10 del Disciplinare ICT e trattamenti dati Revisione 01)

- Il sistema informativo al servizio dell'ambiente, del personale dell'Agenzia, dei cittadini, delle imprese
- Chiunque ha diritto alla protezione dei dati personali
- Sicurezza per salvaguardare il valore delle informazioni, la riservatezza e la continuità operativa
- Integrazione, aderenza agli standard, open source
- Efficacia, efficienza, competenza, iniziativa, collaborazione, interscambiabilità, razionalizzazione
- Segreto di ufficio, riservatezza nelle istruttorie, divulgazione delle informazioni di interesse pubblico

Estensore: Ing. Mario Daddi

Proponente: Dott. Marco Chini

Approvazione: Ing. Marcello Mossa Verre

tel. 055.32061 - fax 055.3206324 - p.iva 04686190481 - www.arpat.toscana.it

per comunicazioni ufficiali PEC: arpat.protocollo@postacert.toscana.it - (accetta solo PEC),
per informazioni ambientali: urp@arpat.toscana.it

Indice generale

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

1. Licenza d'uso

2. Finalità dell'utilizzo dei sistemi ICT

L'utilizzo dei sistemi ICT risponde alle seguenti finalità:

1. attuazione della missione di ARPAT;
2. miglioramento dei servizi;
3. trasparenza dell’azione amministrativa;
4. potenziamento dei supporti conoscitivi per le decisioni pubbliche;
5. contenimento dei costi dell’azione amministrativa.

3. Finalità dello sviluppo dei sistemi ICT

Lo sviluppo dei sistemi ICT risponde ai seguenti criteri:

1. attuazione della missione di ARPAT;
2. conseguimento degli obiettivi di informatizzazione stabiliti dal Governo Italiano, quali ad esempio:
    - piano triennale vigente per l’informatica nella pubblica amministrazione;

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- attuazione delle politiche intese ad assicurare la trasparenza, intesa come accessibilità totale delle informazioni concernenti l'organizzazione e la attività di ARPAT, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche;
- completa informatizzazione delle procedure per la presentazione di istanze, dichiarazioni e segnalazioni che possono essere inoltrate ad ARPAT da cittadini e imprese;
- utilizzo di strumenti per la valutazione immediata continua e sicura del giudizio degli utenti che utilizzano i servizi di rete erogati da ARPAT;
- obbligo di rendere accessibili in ogni momento agli interessati, tramite gli strumenti di identificazione informatica di cui all'articolo 65, comma 1 del Codice dell'Amministrazione Digitale (ovvero Carta di identità elettronica, CNS e SPID), le informazioni relative ai procedimenti amministrativi che li riguardano, ivi comprese quelle relative allo stato della procedura, ai relativi tempi e allo specifico ufficio competente in ogni singola fase;
- fatturazione elettronica, pagamenti elettronici, conservazione sostitutiva;
- riuso del software, utilizzo di software liberi o a codici sorgente aperto;

3. razionalizzazione, al fine di poter ridurre i costi e migliorare i servizi erogati;
4. integrazione ed interconnessione dei sistemi medesimi;
5. attuazione del controllo direzionale (pianificazione, contabilizzazione, controllo di gestione, supporto alle decisioni);
6. aumento della produttività del personale;
7. sicurezza delle informazioni gestite e tutela della privacy;
8. favorire l'accesso ai servizi erogati, anche ai diversamente abili (accessibilità);
9. rispetto degli standard definiti anche in armonia con le normative comunitarie adottando ove possibile soluzioni open source;
10. collegamento con il sistema statistico regionale e nazionale.

4. Finalità della gestione del livello di riservatezza dei dati, documenti e informazioni

La gestione del livello di riservatezza dei dati, documenti e informazioni è finalizzata da una parte a proteggere informazioni riservate, dall'altra a promuovere la diffusione di tutte le informazioni di possibile interesse pubblico attraverso i canali previsti. A tal fine risponde ai seguenti criteri:

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

1. i trattamenti dei dati personali si effettuano nelle modalità previste dal Codice Privacy e Regolamento (UE) 679/2016, nel rispetto dei seguenti principi generali:
   a) protezione dei diritti e delle libertà fondamentali degli interessati, con riferimento alla protezione dei dati personali, al diritto di accesso e agli altri diritti degli interessati;
   b) minimizzazione dei dati: sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   c) limitazione della conservazione: sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate, richieste dal Regolamento (UE) 679/2016 a tutela dei diritti e delle libertà dell'interessato;
2. dovere di segretezza nell'esercizio dell'attività amministrativa, sanzionatoria e di tutela amministrativa e giudiziaria, al fine di evitare che ARPAT possa subire un pregiudizio sotto il profilo del "regolare funzionamento della sua attività", nonché allo scopo di impedire che soggetti esterni possano trarre ingiusto profitto dalle conoscenze acquisite;
3. diritto di accesso agli "Atti Amministrativi" e alle informazioni ambientali da parte di cittadini, società e associazioni, secondo il vigente "Regolamento in materia di procedimento amministrativo e per l'esercizio del diritto di accesso ai documenti amministrativi ed alle informazioni ambientali";
4. illustrare e favorire la conoscenza delle disposizioni normative, al fine di facilitarne l'applicazione;
5. illustrare le attività di ARPAT ed il suo funzionamento;
6. favorire l'accesso ai servizi erogati promuovendone la conoscenza;
7. promuovere conoscenze allargate e approfondite su temi di rilevante interesse pubblico e sociale;
8. favorire processi interni di semplificazione delle procedure e di modernizzazione degli apparati nonché la conoscenza dell'avvio e del percorso dei procedimenti amministrativi;
9. promuovere l'immagine di ARPAT in Italia, in Europa e nel mondo, conferendo conoscenza e visibilità ad eventi d'importanza locale, regionale, nazionale ed internazionale.

5. Politiche di sviluppo e gestione dei sistemi ICT

ARPAT provvede di norma con proprio personale alla progettazione, allo sviluppo e alla gestione dei propri sistemi informativi automatizzati per il conseguimento delle finalità sopra descritte.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Ove sussistano particolari necessità di natura tecnica, adeguatamente motivate, può conferire affidamenti a terzi.

ARPAT tende, nello sviluppo e gestione dei sistemi ICT, all'adozione delle pratiche ottimali (Best Practice) per conseguire i massimi livelli di efficacia ed efficienza.

A tal fine valorizza i seguenti comportamenti, che vengono richiesti al personale addetto:

- acquisizione, anche in autonomia, di adeguate e sempre maggiori competenze sulle tecnologie in uso;
- spirito di iniziativa e di collaborazione, nel rispetto di procedure e regole, per operare al meglio in team;
- interscambiabilità e razionalizzazione, per assicurare la continuità dei servizi;
- contabilizzazione delle attività, per contribuire al meglio alla programmazione e al conseguimento di una sempre maggiore razionalizzazione.

6. Politiche di sicurezza

6.1 Modalità di gestione della sicurezza

Le informazioni gestite dal sistema informativo di ARPAT e lo stesso sistema informativo costituiscono una risorsa di valore strategico per l'Agenzia e per il governo del Paese.

Questo patrimonio deve essere efficacemente protetto e tutelato per:

- motivi economici, ovvero per ridurre il rischio di perdita informazioni preziose (che sono costate moltissime ore di lavoro) e di fermo dei servizi (su cui si basa l'efficienza di ARPAT e l'espletamento dei suoi compiti istituzionali);
- assicurare la protezione di informazioni riservate.

La protezione delle informazioni e la continuità operativa si basa sulla adozione della seguente modalità di gestione della sicurezza:

a) analisi dei rischi che incombono sui dati;

b) definizione di specifiche misure di sicurezza che consentano di ridurre il rischio a un livello giudicato accettabile, in funzione dei seguenti elementi considerati nel loro insieme:
   - valore dei beni da proteggere (informazioni e servizi);
   - potenziali minacce e vulnerabilità dei beni da proteggere;
   - possibile danno derivante dall'accesso non autorizzato o dall'interruzione dei servizi;
   - necessità di rispettare le misure minime di sicurezza previste dalla normativa vigente (Codice Privacy, Codice dell'amministrazione digitale, Direttiva sicurezza, ecc.);

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- necessità di operare nel rispetto dei principi di semplificazione, efficienza ed efficacia.

c) monitoraggio periodico delle criticità presenti mediante redazione annuale di una relazione sull'ICT, approvata dal Titolare, che descriva i servizi erogati, gli SLA garantiti, le criticità connesse alla sicurezza ICT e le misure adottabili per la loro risoluzione;

d) programmazione delle attività che riguardano la sicurezza nell'ambito dei piani annuali esercizio, investimento, attività, formazione, qualità, che vengono approvati dopo valutazione delle criticità descritte nella relazione sulla sicurezza.

6.2 Analisi dei rischi

Di seguito i principali eventi potenzialmente dannosi per la sicurezza dei dati:

6.2.1 Comportamenti degli operatori

1. sottrazione di credenziali di autenticazione;
2. carenza di consapevolezza, disattenzione o incuria;
3. comportamenti sleali o fraudolenti;
4. errore materiale.

6.2.2 Eventi relativi agli strumenti

1. azioni di virus informatici o di programmi suscettibili di recare danno;
2. spamming o tecniche di sabotaggio;
3. malfunzionamento, indisponibilità o degrado degli strumenti;
4. accessi interni o esterni non autorizzati;
5. intercettazione di informazioni in rete;

6.2.3 Eventi relativi al contesto fisico ambientale

1. ingressi non autorizzati a locali/aree ad accesso ristretto;
2. sottrazione di strumenti contenenti dati;
3. eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti all'incuria;
4. guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.);
5. errori umani nella gestione della sicurezza fisica.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

6.3 Misure di sicurezza per garantire la riservatezza, l'integrità e la disponibilità dei dati

Nel presente paragrafo sono riportate le misure di sicurezza da adottare per assicurare la riduzione di tutte le tipologie di rischio individuate al paragrafo precedente.

Includono:

- misure minime previste dalla normativa sulla Privacy;
- misure minime di sicurezza ICT per contrastare la minaccia cibernetica, prescritte dal Governo Italiano alle Pubbliche Amministrazioni con Circolare AGID N. 2/2017, in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015, riportate nei paragrafi 6.3.5 – 6.3.12, che includono:
  - misure di "livello minimo", obbligatorie per tutte le PA;
  - misure di "livello standard", cui tutte le PA dovrebbero tendere;
  - misure di "livello alto", da implementare per conseguire un maggiore livello di sicurezza.

  Occorre implementare prioritariamente le misure di livello minimo e standard e, successivamente, verificare la possibilità di implementare quelle di livello alto (non riportate nel presente documento, salvo quelle necessarie subito);
- adempimenti di altre normative.

6.3.1 Misure generali di sicurezza

Una prima riduzione complessiva dei rischi che incombono sui dati si basa sulla redazione, aggiornamento e diffusione del "Disciplinare ICT e trattamenti dati", che costituisce un unico riferimento normativo per comunicare a coloro che utilizzano i sistemi ICT (incaricati) e ai Responsabili:

- le corrette modalità per l'utilizzo degli strumenti ICT aziendali loro assegnati;
- le modalità su cui si basa la distribuzione dei compiti e delle responsabilità nella gestione e utilizzo del sistema informativo;
- le modalità adottate per il monitoraggio dei sistemi ICT;
- le modalità adottate per regolamentare l'utilizzo e la gestione dei sistemi ICT, anche allo scopo di assicurare continuità operativa;
- le modalità adottate per assicurare la formazione degli incaricati;
- le norme generali di comportamento prescritte a tutti gli incaricati;
- le modalità per i controlli e le sanzioni.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

6.3.2 Gestione della riservatezza dei dati

Si basa sulle seguenti misure minime di sicurezza:

1. identificazione, da parte dei Responsabili, del livello di riservatezza dei dati gestiti in funzione delle seguenti tipologie:
   - dati pubblici, di libera consultazione da parte del personale interno ed esterno, destinati alla diffusione tramite il sito istituzionale;
   - dati interni, di libera consultazione da parte del personale interno e da parte del personale esterno che accede alla intranet, destinati alla diffusione tramite la intranet;
   - dati riservati (dati personali comuni riservati, dati personali sensibili e giudiziari, altre tipologie di dati riservati), che possono essere trattati dal solo personale autorizzato tramite un sistema applicativo dotato di sistema di autorizzazione;
2. protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, con messa in atto, per i dati riservati, di misure tecniche e organizzative adeguate, quali la pseudonimizzazione, impostazioni predefinite che limitino i trattamenti in funzione delle specifiche diverse finalità e che evitino che i dati riservati siano resi accessibili a un indefinito numero di persone fisiche senza l'intervento della persona fisica (le limitazioni dei trattamenti riguardano la quantità di dati raccolti, la portata del trattamento, il periodo di conservazione, l'accessibilità);
3. identificazione, nell'ambito delle schede sistema, delle tipologie di dati che possono essere trattate nei singoli sistemi ICT e descrizione delle modalità di trattamento;
4. designazione, da parte dei competenti Responsabili, degli incaricati autorizzati al trattamento dei dati;
5. attuazione di politiche per la gestione degli accessi degli utenti ai sistemi applicativi (vedi paragrafo successivo);
6. formazione dei Responsabili e degli incaricati al fine di assicurare il rispetto delle misure minime di sicurezza definite nell'Allegato 2 del Disciplinare (norme generali di comportamento);
7. identificazione, nell'ambito dei sistemi applicativi, dei soggetti cui si riferiscono i dati trattati, anche al fine di poter assicurare i diritti di accesso degli interessati previsti dalla normativa sulla privacy (art. 7 del Codice Privacy e art. 15 del Regolamento (UE) 679/2016) e dalle disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione (Legge 190/2012, comma 30);
8. conservazione dei dati sui supporti di memorizzazione dei server, i quali sono ubicati in aree protette e sono configurati per assicurare elevato livello di protezione dei dati stessi;
9. divieto di esportare banche dati che contengono informazioni riservate all'esterno dei locali del centro elaborazione dati di ARPAT (salvo preventiva crittografia o tecniche analoghe finalizzate a renderli non intelligibili); se le informazioni riservate sono gestite

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

come servizi in outsourcing, è necessario verificare che la società che eroga il servizio per conto di ARPAT ne effettui la gestione nel pieno rispetto della normativa sulla privacy.

6.3.3 Gestione degli accessi delle/degli utenti ai sistemi applicativi

Gli accessi delle/degli utenti ai sistemi applicativi sono differenziati in funzione del rapporto di lavoro / contrattuale / di collaborazione che sussiste tra il personale interessato e l'Agenzia.

1. Personale che ha un rapporto di lavoro con l'Agenzia: i diritti di accesso ai sistemi applicativi sono stabiliti dal Responsabile della struttura cui l'utente è assegnato e sono legati alla presenza di un rapporto di lavoro con l'Agenzia.

   Alla cessazione del rapporto di lavoro sono rimossi tutti i diritti di accesso ai sistemi applicativi di ARPAT.

   A seguito del trasferimento ad altra struttura dell'Agenzia sono rimossi tutti i diritti di accesso ai sistemi applicativi, con la sola esclusione dei servizi garantiti a tutti i dipendenti ARPAT, quali ad esempio casella di posta elettronica, condivisione personale, accesso ai contenuti pubblici della intranet e del sistema di protocollo informatico e gestione documentale.

   Le credenziali di autorizzazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

2. Altro personale: i diritti di accesso sono stabiliti dal Responsabile che ne ha in carico la gestione, in funzione della presenza di un accordo contrattuale con l'azienda/società cui l'utente appartiene o di un accordo di collaborazione con la pubblica amministrazione cui l'utente appartiene o con l'utente stessa/o (esempio stage, consulenze, ecc.).

   I diritti di accesso sono rimossi alla data di cessazione degli accordi contrattuali o di collaborazione.

   Le credenziali di autorizzazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

6.3.4 Gestione dei beni ICT

Si applica quanto segue:

1. inventariazione dei beni ICT;
2. definizione delle responsabilità di gestione e controllo;
3. definizione delle regole di corretto utilizzo;
4. restituzione degli strumenti e apparecchiature ICT alla cessazione dell'esigenza per la quale erano state previste (ad esempio alla cessazione dell'incarico, del rapporto di lavoro, del rapporto di collaborazione, del rapporto contrattuale con ARPAT o a seguito di trasferimento presso altra struttura di ARPAT).

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

6.3.5 Inventario dei dispositivi di rete autorizzati e non autorizzati

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso:

1. Implementare un inventario delle risorse attive correlato all'inventario di tutti i sistemi e dispositivi di rete di cui al successivo punto 3 e assicurarne l'aggiornamento quando nuovi dispositivi approvati vengono collegati in rete.

   Implementare l''inventario attraverso uno strumento automatico (livello standard).

2. Implementare il "logging" delle operazioni del server DHCP. Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite (livello standard).

3. Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

   Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale (livello standard).

6.3.6 Inventario dei software autorizzati e non autorizzati

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione.

1. Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.

   Per conseguire il livello standard occorre inoltre:

   - Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.
   - Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", isolare il software personalizzato in un sistema operativo virtuale applicando la misura sottoriportata.
   - Utilizzare macchine virtuali e/o sistemi air-gapped (cioè isolati) per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete (livello alto).

- Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.

2. Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

6.3.7 Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

1. Definire e impiegare configurazioni sicure standard per la protezione dei sistemi operativi per workstation, server e altri tipi di sistemi usati dall'organizzazione.

   Per conseguire il livello standard:

   - Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
   - Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.

2. Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3. Le immagini d'installazione devono essere memorizzate offline.

   Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati (livello standard).

4. Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).
5. Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati (livello standard).

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

6.3.8 Valutazione e correzione continua della vulnerabilità (ricerca delle vulnerabilità, aggiornamenti del software e del sistema operativo)

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

(I) Ricerca delle vulnerabilità

1. A ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
2. Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
3. Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4. Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
5. Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.

Livello standard:

6. Eseguire periodicamente la ricerca delle vulnerabilità di cui sopra, con frequenza commisurata alla complessità dell'infrastruttura.
7. Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.
8. Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità.
9. Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.
10. Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.
11. Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

12. Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzarle per aggiornare le attività di scansione (livello standard).

(II) Aggiornamenti del software e del sistema operativo

1. Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.
2. Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
3. Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4. Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
5. Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.

Livello standard:

6. Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.
7. Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.
8. Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.
9. Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.

6.3.9 Uso appropriato dei privilegi di amministratore

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

1. Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
2. Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

3. Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
4. Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5. Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (ad esempio almeno 14 caratteri).
6. Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
7. Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
8. Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
9. Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
10. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
11. Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
12. Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

Livello standard:

13. Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
14. Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.
15. Generare un'allerta quando viene aggiunta un'utenza amministrativa.
16. Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.
17. Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
18. Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
19. Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
20. Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

21. Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.
22. Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.
23. Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).

6.3.10 Difese contro i malware

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.

1. Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
2. Installare su tutti i dispositivi firewall ed IPS personali.
3. Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
4. Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
5. Disattivare l'esecuzione automatica dei contenuti dinamici (ad esempio macro) presenti nei file.
6. Disattivare l'apertura automatica dei messaggi di posta elettronica.
7. Disattivare l'anteprima automatica dei contenuti dei file.
8. Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
9. Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
10. Filtrare il contenuto del traffico web.
11. Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (ad esempio .cab).

Livello standard:

12. Gli eventi rilevati dagli antivirus locali sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

13. Tutti gli antivirus locali sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.
14. È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi antimalware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.
15. Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.
16. Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.
17. Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
18. Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.
19. Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.

6.3.11 Copie di sicurezza

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità in tempi compatibili con la tipologia di servizio erogato e comunque non superiori a 7 giorni.

1. Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
2. Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
3. Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

Livello standard:

4. Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.

Modalità specifiche per ARPAT:

5. **Sistemi di produzione**:

   a) Salvataggio incrementale dei dati almeno giornaliero.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

b) Salvataggio completo dei dati con periodicità definita e compatibile con la tipologia dei servizi ad essi correlati (settimanale, mensile o annuale).

c) Conservazione dei backup su supporti separati dai dischi presenti sui server, in cassaforte ignifuga posta in edificio separato dal centro elaborazione dati.

d) Conservazione degli ultimi 3 salvataggi full per ogni sistema.

e) Almeno un salvataggio completo all'anno, da conservare per almeno un anno.

f) Conservazione dei backup dei documenti degli archivi, delle scritture contabili, della corrispondenza e di ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento per i tempi previsti dalla normativa vigente.

6. **Sistemi di test e collaudo**:

   a) Salvataggio giornaliero senza conservazione dei backup.

6.3.12 Protezione dei dati

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti:

1. Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica (per le modalità vedi anche paragrafo "6.3.2 Gestione della riservatezza dei dati").
2. Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti (livello standard).
3. Bloccare il traffico da e verso url presenti in una blacklist.

6.3.13 Misure di sicurezza per gli applicativi e servizi di rete

Sono dotati di:

1. sistemi per l'accesso degli utenti basati su carta di identità elettronica, carta nazionale dei servizi e SPID (Sistema Pubblico per la gestione delle identità digitale di cittadini e imprese), per tutti i servizi erogati in rete destinati all'esterno di ARPAT. Per i sistemi di nuova attivazione viene utilizzato esclusivamente il sistema SPID;
2. sistemi per l'accesso degli utenti basati sul sistema interno di autenticazione centralizzata, per tutti i servizi erogati in rete destinati al personale interno e al personale esterno che opera nelle strutture di ARPAT;
3. sistemi di autorizzazione, nei casi in cui sia necessario gestire differenti profili di autorizzazione degli utenti;
4. sistema interno di autenticazione centralizzata basato su tecnologia crittografica, configurato per non accettare password più corte di 8 caratteri prive di numeri o caratteri

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

speciali, per obbligare l'utente a cambiare la password al primo utilizzo e successivamente almeno ogni 3 mesi;

5. sistemi per l'identificazione dei soggetti cui si riferiscono i dati trattati, anche al fine di poter attuare quanto previsto dall'art. 7 del Codice Privacy (“Diritto di accesso ai dati personali e altri diritti”), dall’art. 15 del Regolamento (UE) 679/2016 e dalla Legge 190/2012, comma 30;
6. sistemi per assicurare la reportistica dei diritti di accesso degli incaricati, raggruppati per struttura di assegnazione, al fine di semplificare le verifiche annuali dei profili di autorizzazione da parte dei Responsabili;
7. sistemi di monitoraggio delle principali attività degli utenti;
8. funzionalità che richiedano nuovamente l'inserimento della password prima delle operazioni di maggiore criticità;
9. funzionalità che consentano di assicurare la immodificabilità dei dati e documenti di cui è prevista la conservazione per legge o regolamento.

Gli applicativi e i servizi di rete utilizzano:

10. tecnologie che assicurino elevata disponibilità dei servizi e continuità operativa (tecnologie di virtualizzazione, server con dischi in mirror o RAID, storage per i sistemi strategici, gruppi di continuità, configurazioni per lo spegnimento controllato dei server nei casi in cui venga a mancare l’alimentazione della rete elettrica);
11. tecnologie che assicurino un elevato livello di protezione delle banche dati aziendali e continuità operativa (quali, ad esempio, sistemi di firewall/proxy per separare le banche dati presenti su internet (WAN) da quelle utilizzabili in intranet (LAN), protocolli crittografici che permettano una comunicazione sicura dal sorgente al destinatario (end-to-end) su reti TCP/IP, separazione delle banche dati dei sistemi transazionali dalle banche dati per il data warehouse);
12. sistemi per il monitoraggio dei server, dei servizi e degli applicativi strategici (basati sull'utilizzo di un sistema per sincronizzare gli orologi di tutti i sistemi di elaborazione di ARPAT, registrazione delle attività degli utenti, degli amministratori di sistema e degli eventi relativi alla sicurezza in ordine cronologico, sistemi di protezione dei log contro l'alterazione e l'accesso non autorizzato, ecc.);

Per la gestione degli applicativi e dei servizi di rete si utilizzano contratti di assistenza ove non sia possibile assicurare adeguata continuità operativa con personale interno.

6.3.14 Gestione delle infrastrutture di supporto, protezione delle aree e dei locali

Per ridurre i rischi che incombono sui dati di cui ai paragrafi 6.2.2 (escluso 6.2.2.1) e 6.2.3, si applica quanto segue:

1. assicurare che l’accesso nei locali avvenga in modo controllato;

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

2. presenza di servizi di supporto al funzionamento dei sistemi informatici, dimensionati per assicurare sufficiente continuità di funzionamento e tempestiva segnalazione di allarme in caso di necessità (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
3. protezione degli apparati critici (ad esempio server, apparati di rete e altri apparati critici posti in locali o armadi climatizzati, protetti da accessi non autorizzati, dotati di sistemi di allarme e/o antincendio);
4. protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari);
5. utilizzo di tecnologie, per gli apparati per la rete interna, in grado di assicurare elevata sicurezza e continuità operativa (ad esempio apparati dotati di sistemi di gestione integrata e remota delle funzionalità e che non consentano di carpire con “sniffer” le eventuali password passate in chiaro sulla rete; utilizzo di sistemi per il monitoraggio degli apparati di rete).

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it