ARCA JONICA

Agenzia Regionale per la Casa e l'Abitare

PROVINCIA DI TARANTO

"DISCIPLINARE TECNICO"

SUI SISTEMI INFORMATIVI DELL'ENTE
E
DISPOSIZIONI IN MATERIA DI MISURE MINIME DI SICUREZZA

(D.L.vo N. 196/2003 e successive modifiche ed integrazioni)

Il presente documento si compone di n. 35 pagine (inclusa la presente)
e di vari moduli a parte scaricabili dal seguente link "Modulistica"

Data di emissione: 22 settembre 2014

Approvato con Determinazione Direttoriale

N. 64 del 22 settembre 2014

IL Direttore Generale
Titolare della Privacy
f.to Avv. Mauro Leone

SOMMARIO:

Elenco Allegati costituenti parte integrante di questo documento:

- *Quadro riepilogativo delle misure di sicurezza tecniche per i trattamenti senza strumenti elettronici e dei relativi codici.*
- *Modello - richiesta di assistenza tecnica: D.T._MOD.01*
- *Modello - istanza di accesso alla casella di posta elettronica della postazione client: D.T._MOD.02;*
- *Modello - istanza di accesso ai contenuti (file/cartella) della postazione client: D.T._MOD.03;*
- *Modello - Verbale di accesso ai messaggi di posta elettronica da parte dell'amministratore di sistema o del referente informatico esterno: D.T._MOD.04;*
- *Modello - Verbale di accesso* al/alla file/cartella da parte *dell'amministratore di sistema o del referente informatico esterno: D.T._MOD.05;*

ARCA JONICA
Agenzia Regionale per la Casa e l'Abitare
DELLA PROVINCIA DI TARANTO

Via Pitagora, 144/A
74100 Taranto

Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dall'Ente ARCA JONICA della Provincia di Taranto, previsti dal D.L.vo 30/06/2003 N. 196 "Codice in materia di protezione dei dati personali" e successive modificazioni/integrazioni e dalle istruzioni impartite dal Garante della Privacy

Il presente documento è stato realizzato dall'Ufficio Privacy, in collaborazione con la Multimedia System di Salvi Michele.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Normativa di riferimento

- D.L.vo n.196 del 30/06/2003 (**Codice** della Privacy);
- Del. n.13 - 1° marzo 2007 del Garante della Privacy (Linee guida del Garante per l'utilizzo della rete, posta elettronica e internet);
- Provvedimento del 27 novembre 2008 del Garante della Privacy (Amministratori di Sistema)
- l'art. 2 della Legge 17/3/1993 n.63 e il DPCM 5/5/1994 in tema di collegamenti telematici;
- l'art. 2, comma 5 della Legge 15/5/1997 n.127;
- l'art. 43 del D.P.R.28/12/2000 n.445;
- il Dlgs 7/3/2005 n.82 (Codice dell'Amministrazione Digitale)

Definizioni e responsabilità

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

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.

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.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate di seguito nel presente documento.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nell'atto di nomina, ne può assume le funzioni l'amministratore di sistema.

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete e custode delle password, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ha le responsabilità indicate nell'atto di nomina, di quelle indicate più avanti nel presente documento e in breve con i compiti di seguito descritti :

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi con la collaborazione di eventuali tecnici esterni;
- assistere all'operato di eventuali tecnici esterni all'amministrazione;
- fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- gestire le password di root o di amministratore di sistema;
- predisporre, per ogni incaricato del trattamento (qualora nominato) e per ogni Banca Dati, una busta sulla quale è indicato lo User-Id utilizzato e al cui interno è contenuta la Password usata per accedere alla Banca Dati;
- revocare tutte le password non utilizzate per un periodo superiore a 6 mesi;
- revocare tempestivamente tutte le password assegnate a soggetti che su comunicazione scritta del responsabile del trattamento non sono più autorizzati ad accedere ai dati;
- gestire le buste contenenti le password degli incaricati del trattamento e conservarle in un luogo sicuro e protetto;
- collaborare con il responsabile del trattamento dati, informandolo sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali e degli apparati elettronici. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità di cui al D.L.vo n.196 del

30/06/2003 di cui ne assume le funzioni il responsabile del trattamento dati e indicate più avanti nel presente documento.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità di cui al D.L.vo n.196 del 30/06/2003 e di quelle indicate nel presente documento.

TITOLARE: titolare del trattamento dati, la cui titolarità è esercitata dal rappresentante legale. Tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte del Responsabile o Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

Titolare, responsabili, incaricati

Titolare del trattamento: Avv. Mauro Leone (Direttore Generale)

Responsabile del trattamento: Sig. Antonio Marzia

Responsabile della sicurezza informatica: Sig. Antonio Marzia

Amministratore di sistema: Dott. Francesco Gregorio

Custode delle password: Dott. Francesco Gregorio

Responsabile esterno del trattamento dati, dell'assistenza e della manutenzione degli strumenti informatici: Sig. Michele Salvi - Ditta Multimedia System -

Incaricato esterno della sicurezza/vigilanza dell'Ente e della videosorveglianza: Istituto di vigilanza: VIS S.p.a.

Titolo I
A) Trattamento dei dati con strumenti elettronici

1) Struttura del sistema e protezioni

1.1 Architettura della rete

I servizi gestiti dall'Ente "ARCA JONICA" della Provincia di Taranto, sono collegati alla rete in fibra ottica e con linee HDSL.
Tutti i dipendenti dotati di PC, formalmente autorizzati, sono quindi collegati alla rete Intranet dove sarà implementato un Dominio Active Directory.
Da tale rete gli stessi possono accedere ai programmi gestionali dell'Ente quali GELIM e PROGRAMMA PARSEC.
Previa autorizzazione i dipendenti potranno accedere ad Internet tramite un sistema di proxy e firewall aziendale.

1.2 Sicurezza della rete

L'accesso ai programmi avviene tramite autenticazione con nome utente e password.
Tutti gli accessi elencati afferiscono a un sistema di firewall, che controlla il traffico dati in base a politiche di sicurezza prestabilite.

1.3 Architettura del Sistema Informatico

Banche dati
I dati strutturati delle applicazioni gestionali sono/saranno memorizzati in:

- banche dati centralizzate, per le applicazioni utilizzate da più utenti;

Oltre alle banche dati delle applicazioni gestionali esistono archivi documentali non strutturati, residenti su :

- server centrali (file server)
- stazioni di lavoro

Posta elettronica
La posta elettronica viene gestita internamente; ad ogni dipendente è assegnata una casella individuale; inoltre esistono caselle non nominali corrispondenti a gruppi di lavoro o figure istituzionali.

Sistemi di autenticazione
Nell'Ente è presente un sistema centralizzato di autenticazione/autorizzazione, Dominio Windows Active Directory, utilizzato per autenticare gli utenti a risorse condivise su rete come:

- cartelle
- stampanti
- applicativi su server web

Saranno messi a punto meccanismi di aggiornamento e allineamento degli utenti fra i vari sistemi come:

- Le modifiche alla password degli utenti, saranno riportate automaticamente sul dominio Active Directory.

Alcune procedure applicative non utilizzano questo sistema centralizzato, ma possiedono un proprio sistema di autenticazione ed autorizzazione degli utenti.

Ad ogni singolo utente possono essere assegnate più credenziali, diverse fra loro, a seconda delle procedure applicative alle quali accede.

1.4 Sicurezza dei dati

Banche dati centralizzate
L'accesso ai dati avviene tramite le procedure gestionali che li trattano: all'utente viene richiesta la digitazione di username e password. Queste credenziali sono verificate dalla procedura stessa.
Contestualmente viene verificato se l'utente è autorizzato all'utilizzo della funzionalità richiesta.

Archivi documentali centralizzati
Il server contenente archivi documentali richiede l'autenticazione e l'autorizzazione dell'utente, tramite il dominio Active Directory.

Banche dati ed archivi documentali residenti su P.C.

I PC che contengono banche dati locali o archivi documentali, contenenti dati personali e/o sensibili, sono protetti da credenziali di accesso personali, come precedentemente descritto.

2) Modalità di gestione delle credenziali di autenticazione e delle autorizzazioni.

2.1 Incaricati del trattamento informatico.

Sono tutti gli operatori tecnici dell'Ufficio Privacy (Amministratori di sistema e Responsabili del trattamento dati).

2.2 Soggetto preposto alla custodia delle credenziali, alla loro attribuzione, cancellazione, modifica

Preposto alla gestione delle credenziali per l'accesso alle banche dati centralizzate è il Responsabile dell'Ufficio Privacy, tramite il responsabile incaricato "Amministratore di sistema", con funzioni anche di amministratore di rete.

Il preposto alla gestione delle credenziali provvede, ogni sei mesi, a fornire ad ogni Dirigente di Settore l'elenco aggiornato di tutti coloro che, a qualsiasi titolo, sono autorizzati ad accedere alle banche dati di quel Settore .
Il preposto alla gestione delle credenziali può variare la password degli incaricati, in caso che si renda indispensabile ed indifferibile , per esclusiva necessità di operatività e sicurezza del sistema, dandone pronta comunicazione agli stessi in modo riservato.
Nessuna responsabilità può essere addebitata al preposto alla gestione delle credenziali per eventuali ritardi od omissioni a lui non imputabili nella concessione, revoca o modifica delle autorizzazioni.

2.3 Trattamento dei dati personali affidati ai lavoratori

Assegnazione delle credenziali di autenticazione
Le credenziali di autenticazione consistono in un codice per l'autenticazione dell'incaricato (user-id) associato ad una parola chiave riservata (password).

In caso di assunzione di un nuovo lavoratore, per quest'ultimo, il Dirigente del Settore interessato richiede all'Ufficio Privacy l'assegnazione della casella di posta elettronica e delle credenziali di autenticazione. Il preposto alla gestione provvede all'assegnazione della posta elettronica, di user-id e della password provvisoria inserendo le credenziali nella apposita directory del SERVER e comunica le credenziali all'utente in modo riservato. Resta a cura del lavoratore sostituire la password provvisoria con quella definitiva.

Può accadere che, per esigenze di servizio, esistano credenziali d'accesso non legate ad un singolo lavoratore e che possono essere condivise da tutto un gruppo di operatori. Queste credenziali non possono consentire l'accesso a banche dati o documenti contenenti dati personali.

Assegnazione delle autorizzazioni
Per poter accedere, a qualsiasi titolo, alle applicazioni ed alle banche dati dell'Ente occorre essere autorizzati.

L'autorizzazione del singolo lavoratore ad accedere alle banche dati dell'ARCA JONICA, deve essere sempre preceduta dal conferimento dell'incarico al

trattamento dei dati da parte del Responsabile del trattamento dei dati d'intesa con il Titolare del trattamento, vale a dire il Direttore Generale.

La competenza alla richiesta, revoca, modifica delle autorizzazioni è del Dirigente del Settore di appartenenza del lavoratore.

Accesso ad applicazioni e banche dati del Settore di appartenenza

Il Dirigente del Settore di appartenenza del lavoratore, comunica per iscritto, anche via e-mail all'Ufficio Privacy, a quali banche dati il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali abilita il lavoratore alle banche dati di sua competenza e provvede a inoltrare la richiesta ai responsabili degli applicativi per le relative autorizzazioni.

Accesso ad applicazioni e banche dati di altri Settori.

Nel caso che il lavoratore necessiti di accedere a banche dati di un altro Settore, l'incarico dovrà essere dato congiuntamente dal Dirigente del Settore di appartenenza e dal Dirigente di Settore titolare della banca dati utilizzata.
Una volta conferito l'incarico, il Dirigente del Settore di appartenenza richiede per iscritto, anche via e-mail, all'Ufficio Privacy l'abilitazione del lavoratore alle banche dati richieste, attestando che il Dirigente del Settore titolare della banca dati ne è stato informato.
Il preposto alla gestione procede con le modalità indicate al paragrafo precedente .

Cessazione del rapporto di lavoro

Nel caso di cessazione del rapporto lavorativo, il preposto alla gestione delle credenziali, attraverso una procedura automatica, ricava dalla Banca dati centralizzata del Settore Personale il nominativo del lavoratore cessato, ne revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica, e ne informa, per iscritto, anche via e-mail, il responsabile informatico dell'applicazione.

Nel caso di rapporto di collaborazione coordinata e continuativa, di prestazione occasionale, di tirocinio formativo ed in genere in tutti i casi in cui non è possibile ricavare l'informazione dell'avvenuta cessazione in modo automatico dalla Banca dati centralizzata del Settore Personale, spetta al Dirigente del Settore competente comunicare tempestivamente per iscritto, anche via e-mail, all'Ufficio Privacy (al preposto alla gestione delle credenziali) l'avvenuta cessazione del rapporto di lavoro e chiedere la revoca delle relative credenziali e autorizzazioni.
Il preposto alla gestione delle credenziali revoca le credenziali e tutte le autorizzazioni all'accesso, incluso l'indirizzo di posta elettronica e ne informa per iscritto, anche via e-mail, il Dirigente del Settore competente e il responsabile informatico dell'applicazione.

Prima della cessazione del rapporto di lavoro, il lavoratore deve eliminare dal suo PC i documenti e le e-mail che non siano d'interesse del Settore, autorizzando per iscritto il Dirigente ad accedere ai documenti e alle e-mail rimanenti. Il Dirigente del Settore interessato deve prontamente avvisare l'Ufficio Privacy che provvederà al ritiro della stazione di lavoro o comunque a rendere indisponibili i dati legati al profilo del lavoratore dopo averne trattenuto una copia. Entro un mese il Dirigente del Settore interessato può richiedere il recupero delle banche dati e delle e-mail giacenti nella casella di posta disabilitata, esibendo la relativa autorizzazione del lavoratore. Trascorso tale periodo il preposto provvederà all'eliminazione definitiva dei suddetti dati.

Trasferimento del lavoratore

Nel caso di trasferimento presso un altro Settore di un lavoratore, il preposto alla gestione delle credenziali, dopo aver rilevato l'informazione attraverso la Banca dati centralizzata del Settore Personale, provvede a revocare tutte le autorizzazioni all'accesso del lavoratore, ad eccezione dell'indirizzo di posta elettronica, e ne informa per iscritto, anche via e-mail, il responsabile informatico dell'applicazione. Il lavoratore trasferito deve reindirizzare al Settore di provenienza tutta la corrispondenza di posta elettronica di competenza di quest'ultimo.

Il Dirigente del Settore di nuova assegnazione/responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, provvede a richiedere le nuove abilitazioni, anche relative all'accesso a banche dati di un altro Settore, con le stesse modalità previste nel caso di nuova assunzione.

Nel caso di trasferimento di un lavoratore nell'ambito dello stesso Settore, il Dirigente di Settore o responsabile delegato, sulla base del nuovo incarico al trattamento dei dati conferito al lavoratore e delle competenze a quest'ultimo attribuite, comunica per iscritto, anche via e-mail all'Ufficio privacy, al preposto alla gestione delle credenziali le autorizzazioni all'accesso da revocare e le nuove applicazioni, anche relative all'accesso a banche dati di un altro Settore, alle quali il lavoratore è autorizzato ad accedere. Il preposto alla gestione delle credenziali disabilita le autorizzazioni all'accesso da revocare, e per le nuove abilitazioni procede con le modalità previste nel caso di nuova assunzione informandone per iscritto, anche via e-mail, il Dirigente di Settore e il responsabile informatico dell'applicazione.

Nel caso che il trasferimento del lavoratore (ad un altro Settore o nell'ambito dello stesso Settore) comporti il contemporaneo trasferimento del PC, il lavoratore è tenuto a consegnare al Dirigente i dati e le e-mail di interesse del Settore e successivamente a rimuoverli dalla propria stazione di lavoro.
Nel caso invece in cui il trasferimento non comporti il contemporaneo trasferimento del PC, si deve seguire il comportamento previsto per il caso di cessazione del rapporto di lavoro.

2.4 *Trattamento dei dati personali affidati a soggetti esterni*

Sono considerati soggetti esterni tutti quei soggetti che non rientrano nel punto 2.3 (a puro titolo esemplificativo: società, enti, consorzi, professionisti, soggetti pubblici o gestori di pubblici servizi).

La titolarità del trattamento dei dati resta in capo all'Ente ARCA JONICA – TA, nella persona del Direttore Generale quale rappresentante legale.

Il Titolare o, su delega dello stesso, il responsabile del trattamento dati, nomina il responsabile esterno.
Nel caso in cui l'oggetto del contratto o della convenzione comporti l'utilizzazione di applicazioni o banche dati di competenza di più Settori, la designazione del responsabile dovrà essere sottoscritta congiuntamente dal Dirigente del Settore contraente e dai Dirigenti delle banche dati interessate. All'inizio della collaborazione il soggetto esterno responsabile del trattamento fornisce al Dirigente del Settore l'elenco degli incaricati al trattamento dei dati da lui

nominati. Il Dirigente di Settore/ responsabile delegato, comunica per iscritto, anche via e-mail, al preposto alla gestione delle credenziali:

- a quali applicazioni l'incaricato è abilitato, richiedendo altresì, se necessario, l'accesso ad Internet e l'utilizzo della posta elettronica;
- la data di scadenza del contratto/ convenzione, se in suo possesso.

Nel caso in cui l'abilitazione riguardi banche dati di competenza di più Settori, nella comunicazione il Dirigente del Settore contraente dovrà altresì dare atto che i Dirigenti dei Settori interessati sono stati informati della richiesta.

Il preposto alla gestione delle credenziali imposta per l'utente un periodo massimo di validità delle credenziali di dodici mesi (o inferiore se la data di scadenza del contratto/convenzione è antecedente a tale termine). Scaduto il periodo di validità, le credenziali dell'utente, se non intervengono ulteriori comunicazioni, saranno automaticamente disabilitate. Qualora il contratto/convenzione abbia una durata superiore all'anno, il responsabile esterno del trattamento dei dati, al fine di evitare che le credenziali degli incaricati siano automaticamente disabilitate alla scadenza dei dodici mesi, dovrà fornire al Dirigente di Settore, due mesi prima della scadenza delle stesse, l'elenco aggiornato degli incaricati. Il Dirigente di Settore/responsabile delegato, trasmetterà all'Ufficio Privacy - al preposto alla gestione delle credenziali il nuovo elenco in sostituzione di quello precedente, comunicando, nel caso che nell'elenco siano presenti anche nuovi incaricati, le applicazioni a cui questi ultimi sono abilitati e richiedendo, se necessario, l'accesso ad Internet e l'utilizzo della posta elettronica.

2.5 Modalità di gestione delle password

Le password utilizzate nei sistemi di autenticazione Active Directory sono assegnate dal preposto alla gestione delle credenziali dell'Ufficio Privacy all'atto della creazione delle credenziali stesse e vengono comunicate in forma riservata all'utente che al primo utilizzo, provvede alla sostituzione della password assegnata con una conosciuta solo dal medesimo.

Nei sistemi Active Directory è stato impostato un meccanismo automatico di scadenza delle password ogni tre mesi. All'approssimarsi della scadenza l'utente viene avvertito via e-mail

Il lavoratore, qualora dimentichi la password d'accesso al proprio PC, deve rivolgersi all'Ufficio Privacy - responsabile custode delle password - che provvederà, previa identificazione personale, a fornire la busta chiusa contenente la password dell'utente da quest'ultimo fornita, in alternativa l'Ufficio Privacy provvederà tramite l'amministratore di sistema e/o il servizio di assistenza, che si recherà sul posto e consentirà all'utente l'accesso al PC allo scopo di impostare una nuova password.

Qualora l'utente sia stato disabilitato per mancato uso delle credenziali per un periodo di almeno sei mesi, la procedura di riattivazione delle credenziali è quella di cui al successivo punto 2.6

Un utente che non sia stato disabilitato può, in qualsiasi momento, modificare la propria password di posta elettronica, autenticandosi con user-id e vecchia password (valida **solo** per questa funzione anche se scaduta): la nuova password verrà scelta dall'utente.

Ogni incaricato che riceve le proprie password ne è direttamente responsabile. Fatta eccezione per quanto previsto dal paragrafo 3.3, il lavoratore non deve in alcun modo comunicare le proprie password a persone diverse od altri incaricati; qualora avesse il timore che la propria password sia divenuta di conoscenza di altri soggetti deve prontamente provvedere a modificarla.

2.6 *Disattivazione credenziali per disuso*

Il mancato uso delle credenziali per almeno sei mesi continuativi determina la loro disattivazione.
Il Dirigente di Settore/responsabile delegato, qualora ritenga di dover riattivare nuovamente le credenziali dell'utente, dovrà chiedere per iscritto, anche via e-mail, all'Ufficio Privacy (al preposto alla gestione delle credenziali) il ripristino delle stesse.
L'utente dovrà rivolgersi all'Ufficio Privacy che provvederà, previa identificazione personale, a fornire in busta chiusa una password provvisoria che consentirà di accedere alla procedura di modifica della password.

3) Modalità di gestione delle stazioni di lavoro

3.1 Soggetto preposto alla cancellazione o recupero delle banche dati su PC

La cancellazione o recupero delle banche dati su PC è competenza dell'Ufficio Privacy, il Responsabile provvederà alla designazione del personale incaricato all'esecuzione.

3.2 Programmi antivirus e Sistemi Operativi

Su tutti i PC saranno installati Sistemi Operativi licenziati che rilasciano aggiornamenti e programmi antivirus non di tipo free che vengono aggiornati periodicamente in modo automatico, tramite l'accesso in rete al Server di gestione antivirus.
L'antivirus installato sui singoli PC controlla in tempo reale l'obsolescenza degli aggiornamenti.

Oltre che sulle stazioni di lavoro è installato un sistema antivirus sul Server per filtrare la navigazione.
Il sistema antivirus installato sul Server di Gestione si aggiorna in modo automatico e contemporaneamente aggiorna l'antivirus installato sulle Postazioni DiLavoro.
E' opportuno che ogni singolo utente, con periodicità almeno quindicinale, effettui con il software antivirus una scansione completa dei dischi interni della stazione di lavoro.

Resta a cura della ditta incaricata della manutenzione dei PC e del Server dell'Ente, formulare un apposto elenco di tutti i Sistemi Operativi e gli Antivirus installati su tutti i PC in dotazione all'Ente Arca Jonica, apponendo analiticamente la data dell'avvenuta installazione del Sistema Operativo, dell'Antivirus e della sua data di scadenza. Tale elenco, costantemente aggiornato, sarà dato in consegna al Responsabile dell'Ufficio Privacy che nell'approssimarsi di ogni scadenza di un Antivirus installato su PC, ne darà subito comunicazione al Dirigente responsabile dell'ufficio che ha in dotazione il PC e provvedendo

contestualmente a darne comunicazione all'Ufficio Economato per il relativo acquisto.

3.3 Interventi di accesso, manutenzione e assistenza a PC e Periferiche

Tutti gli interventi di Manutenzione e le segnalazione di assistenza dovranno essere richiesti dai lavoratori al Responsabile Preposto della Sicurezza Informatica, per consentire di determinarne la gravità e attivare la procedura di intervento, avendo cura di indicare il numero di matricola del PC e/o della periferica interessata alla manutenzione.
Si specifica che per ogni intervento di manutenzione, sarà redatto a cura della ditta incaricata della manutenzione, un apposito rapporto di intervento tecnico, sottoscritto dal Responsabile per la sicurezza informatica dell'Ente e da un incaricato della Ditta, nel quale dovranno essere registrati: l'ufficio interessato, il nominativo del dipendente che ha in dotazione il PC il numero progressivo assegnato cui si riferisce l'apparecchiatura per la quale è stato richiesto l'intervento, il numero seriale, il numero di installazione, il numero di ticket, la data e l'ora della chiamata, il numero dell'intervento, la data e l'ora dell'intervento, la data e l'ora dell'avvenuto ripristino delle funzionalità dell'apparecchiatura (o del termine intervento).
Il modulo di Manutenzione riporterà la descrizione del problema segnalato, il recapito di consegna, come pure il nome del Responsabile interno all'Ufficio Privacy cui la Ditta dovrà rivolgersi.
Ogni modulo di Manutenzione dovrà contenere l'indicazione del personal computer e/o della periferica; in aggiunta sarà possibile specificare, all'interno del medesimo Modulo, dispositivi e servizi richiesti.

Richiesta di accesso
Durante l'assenza del lavoratore il Dirigente del Settore o il responsabile delegato può accedere a dati e procedure del pc del lavoratore assente e verificare il contenuto dei messaggi (esclusivamente sull'indirizzo di posta istituzionale) a quest'ultimo indirizzati, a condizione che ciò si renda indispensabile e indifferibile, per esclusiva necessità di operatività, sicurezza o per improrogabili necessità legate all'attività lavorativa. Ciò deve avvenire, effettuando preventiva comunicazione all'Ufficio Privacy, motivando l'esigenza di accesso ai dati e richiesta della password.

A tale scopo ogni lavoratore deve consegnare all'Ufficio Privacy per iscritto, una busta chiusa contenente le proprie password e/o le credenziali di accesso al sistema, avendo cura di sostituirle ogni volta che esse vengono cambiate.

L'Ufficio Privacy, dovrà custodire in apposita cassaforte o armadio di sicurezza ignifugo, le buste contenenti le credenziali di accesso e le password dei dipendenti, avendo cura di consegnare al Direttore Generale una copia della chiave della cassaforte in caso di assenza del Responsabile Privacy.

Si individuerà un lavoratore in servizio che, su richiesta e alla presenza del Dirigente del Settore/Responsabile incaricato o di un incaricato dell'Ufficio Privacy, dopo aver ricevuto le relative password da quest'ultimo, accede ai dati e alle procedure nonché ai messaggi di posta elettronica del lavoratore assente, provvedendo a inoltrare a chi di competenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Dell'attività compiuta, è redatto apposito verbale a cura del Dirigente/Responsabile delegato, che ne informa il lavoratore assente alla prima occasione utile.

Nel caso in cui non sia possibile servirsi della procedura descritta, il Dirigente del Settore/Responsabile delegato, autorizza e richiede al responsabile dell'Ufficio Privacy l'intervento dell'amministratore di sistema e/o dei tecnici del servizio di assistenza, che ne permettono l'accesso per il tempo necessario.

L'intervento verrà documentato mediante apposito verbale redatto a cura del Dirigente del Settore/Responsabile delegato e comunicato al lavoratore alla prima occasione utile.

Gli interventi dei tecnici addetti all'assistenza dei PC possono avvenire senza conoscere e senza modificare la password del lavoratore, grazie ad una password di servizio custodita dal preposto dell'Ufficio Privacy, secondo le regole tecniche previste dalla legge.

Interventi di Manutenzione
Quando per un PC occorre fare un intervento di manutenzione, ordinaria o straordinaria, sul loco o in laboratorio, sarà cura dell'Ufficio Privacy concordare modi e tempi d'intervento con i tecnici addetti.

3.4 Società esterne o professionisti per la manutenzione e l'assistenza

Il Titolare o il Responsabile della Privacy, nomina per la società che effettua la manutenzione dei sistemi hardware e software dell'Ente il Responsabile esterno del trattamento dati, limitatamente alle istruzioni impartite dall'Ufficio Privacy e Sicurezza, il quale a sua volta nominerà - senza alcun compenso aggiuntivo - i tecnici incaricati esterni al trattamento dati dandone comunicazione scritta al Responsabile della Privacy. Dette nomine comprendono una specifica assunzione di impegno da parte del responsabile e degli incaricati, al rispetto delle seguenti disposizioni:
a) non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'ente detenuti;
b) informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici;
c) richiedere preventivamente l'autorizzazione al responsabile dell'Ufficio Privacy nel caso di interventi di assistenza tramite collegamento remoto. Lo stesso responsabile dell'Ufficio Privacy dovrà essere avvisato al termine delle operazioni.
d) usare riservatezza su dati ed informazioni addivenuti in loro possesso;
e) trasmettere al Responsabile dell'Ufficio Privacy, all'inizio della collaborazione e successivamente ad ogni variazione, l'elenco aggiornato degli incaricati esterni al trattamento.
f) nel caso che gli incaricati, per svolgere la propria attività, necessitino di accedere ad uffici e locali dell'Ente Arca Jonica, si dovrà informare in ogni caso tempestivamente l'Ufficio Privacy di ogni revoca e di ogni nuovo incarico conferito.

3.5 Dismissione

In caso di dismissione di vecchi PC, il Dirigente che ha in carico la stazione di lavoro deve comunicare al responsabile dell'Ufficio Privacy di informare il soggetto preposto alla pulizia la presenza di banche dati da recuperare. Il soggetto preposto

una volta recuperate le banche dati, conserva la stazione di lavoro per un mese quindi provvede a rendere illeggibili i dischi magnetici prima della rottamazione.

4) Salvataggio dei dati

Il salvataggio delle banche dati esistenti sul Server è in carico all' Ufficio Privacy.
Sul sistema centralizzato vengono fatte copie quotidiane in modalità RAID1 degli archivi documentali e delle banche dati strutturate allo scopo di fornire almeno una versione aggiornata alla notte precedente. Altresì mediante un sistema NAS, verrà fatta una ulteriore copia dei dati in modo automatizzato. Da ultimo, cosi come espressamente previsto dall'art. 55bis del CAD, sarà attivata apposita procedura di DISASTER RECOVERY per consentire all'Ente Arca Jonica il ripristino della funzionalità minime dei servizi, nell'arco delle 24 ore successive all'eventuale disastro verificatosi.
Le copie dei dati vengono effettuate su disco rigidio ad alta capacità contenute all'interno del SERVER, e l'altro di backup su NAS entrambi collocati in apposita stanza all'interno del CED. La procedura di DISASTER RECOVERY avviene presso una sede remota.
L'esecuzione dell'operazione di salvataggio è verificata quotidianamente dal gruppo di lavoro dell'Ufficio Privacy.

Ogni singolo lavoratore è responsabile del salvataggio degli archivi esistenti sul proprio PC.

Le banche dati residenti solo sul singolo PC (escludendo pertanto, ad esempio, le banche dati che il lavoratore ha creato per esigenze di funzionalità, quelle di cui esiste una copia cartacea ed in genere, quelle che è possibile ricostruire attingendo ad altre banche dati) sono copiate su apposita directory allocata sul Server.

5) Locali macchine

I locali dove risiedono fisicamente il Server ed il sistema NAS sono dotati di alcuni accorgimenti minimi a garanzia sia della sicurezza fisica dell'hardware, sia delle banche dati:

1. chiusura di sicurezza per la porta di ingresso ai locali, ed accesso controllato per i dipendenti autorizzati;
2. stabilizzatore di temperatura per i locali;
3. gruppo di continuità e di stabilizzazione della corrente;
4. cassaforte ignifuga o armadio per dischetti e CD di salvataggio;
5. impianto di rilevamento fumi e spegnimento automatico in caso di incendio, collegato con la sede di una società di sicurezza e pronto intervento;
6. impianto antintrusione collegato con la sede di una società di sicurezza e pronto intervento

Titolo II
B) Trattamento dei dati senza l'ausilio di strumenti elettronici

6) Osservanze al trattamento dei dati

Il trattamento "cartaceo" di dati personali deve essere garantito da particolari misure minime di sicurezza che debbono essere specificate dal Titolare del

Trattamento dati o dal Responsabile agli incaricati per le diverse tipologie di trattamento.

6.1 Osservanze del responsabile -

- coordinare tutte le operazioni di trattamento dei dati e vigilare sull'osservanza delle istruzioni impartite;
- curare l'informazione agli interessati relativa al trattamento dei dati e alla loro comunicazione;
- assegnare agli incaricati del trattamento le istruzioni per la corretta raccolta, elaborazione, consultazione e custodia dei dati;
- rettificare i dati su richiesta dell'interessato o d'ufficio, quando necessario;
- impartire le disposizioni operative per la sicurezza dell'accesso ai dati e ai documenti;
- curare l'eventuale relazione tra il trattamento effettuato e le singole banche dati gestite dall'Ufficio Privacy;
- formulare proposte per l'eventuale distruzione, se consentito dalle norme, dei documenti contenenti dati non più necessari.
- a tal proposito, ad ogni singolo ufficio verrà consegnato apposito distruggi documenti onde evitare di semplicemente cestinare e quindi rendere sempre leggibili documenti tutelati dalla Privacy

6.2 Osservanze dell'incaricato -

- trattare i dati esclusivamente per gli scopi definiti dall'ambito di trattamento assegnato. I dati non possono in alcun modo essere comunicati a terzi non incaricati;
- osservare le norme di diligenza, prudenza e cautela per prevenire lo smarrimento, la distruzione o la perdita di documenti contenenti dati personali, e per prevenire l'accesso o il trattamento da parte di persone non autorizzate;
- assicurare la custodia delle chiavi di locali, armadi e cassettiere in cui sono conservati i documenti contenenti dati sensibili o giudiziari e, in caso di furto o smarrimento, fare pronta denuncia al responsabile;
- in caso di assenza dall'ufficio per cui il medesimo risulti non presidiato, proteggere in luogo custodito i singoli documenti temporaneamente estratti dall'archivio per motivi di lavoro e non lasciarli sulle scrivanie o alla libera visione di terzi;
- evitare di effettuare il trattamento dei dati personali in presenza di terzi che possano così venire a conoscenza, anche occasionalmente, dei dati.

Titolo III
C) Piano programmatico sulle misure si sicurezza

Il presente documento, considerate le caratteristiche organizzative dell'Ente, rinvia alcuni adempimenti alle determinazioni che l'Ufficio Privacy dovrà adottare e precisamente:

- L'analisi dei rischi che incombono sui dati;
- Le misure ulteriori da adottare, aggiuntive rispetto a quelle indicate e descritte nei punti seguenti, per garantire l'integrità e la disponibilità dei dati.

- Il Servizio/Ufficio/Responsabile preposto, dovrà garantire la protezione delle aree e dei locali, con specifico riferimento ai Piani di Emergenza elaborati per le diverse Strutture dell'Ente.

- Il Servizio/Ufficio/Responsabile preposto, dovrà provvedere alle autorizzazioni ad accedere ai locali al di fuori dell'orario di lavoro del personale dell'impresa di pulizia per le sedi oggetto di appalto.

- L'accesso nell'Ente dopo l'orario di chiusura sarà garantito dal personale di sorveglianza, gestito dal Servizio/Ufficio/Responsabile preposto, a mezzo di strumenti di Videosorveglianza degli accessi.

Il sistema di videosorveglianza degli accessi deve essere installato, rispettando tutte le disposizioni di legge in materia di privacy e tutela dei dipendenti, solo dopo avvenuta ricezione di autorizzazione del Ministero del Lavoro inoltrata all'ufficio provinciale del lavoro di Taranto con apposita pratica ed iter previsto per legge.

- L'accesso dopo l'orario di chiusura nell'edificio, sede degli uffici di Via Pitagora e Via Regina Elena , è consentito con apposita autorizzazione a dirigenti, funzionari e lavoratori, titolari di apposito badge identificativo personale che attiva il dispositivo marcatempo.

- L'Ufficio Privacy dovrà curare la formazione dei dipendenti con corsi in special modo nei confronti dei nuovi assunti. In modo particolare il programma di formazione dovrà :

a) rendere consapevoli i partecipanti sull'importanza delle scelte dell'Ente;
b) coinvolgere i partecipanti sulle problematiche inerenti la sicurezza;
c) responsabilizzare i partecipanti sulle attività da eseguire.

I corsi saranno progettati in base alle diverse esigenze ed ai diversi sistemi di sicurezza sviluppati, in funzione al grado di informatizzazione raggiunto.
In generale non potranno mancare riferimenti a:

- normativa vigente;
- definizione delle responsabilità;
- elenco delle vulnerabilità: spesso non c'è la consapevolezza dei rischi che si possono correre.
- regole comportamentali che comprendono la gestione degli accessi (password.);
- regole comportamentali di riservatezza sia in orario di lavoro sia al di fuori dell'ambito lavorativo;
- i possibili rischi: virus, intercettazioni, intrusioni, ecc..

- Sarà elaborato un piano affinché ogni Settore provvederà:
  - alla conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale, dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo;
  - all'adozione di codici identificativi o soluzioni analoghe che rendano i dati sensibili e giudiziari contenuti in elenchi, registri, banche dati tenuti con l'ausilio di strumenti elettronici temporaneamente inintelleggibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Per tale attività i Settori si avvalgono, qualora lo ritengano opportuno, dell'ausilio dell'Ufficio Privacy.

- L'Ente Arca Jonica di Taranto sarà impegnato in un processo di valorizzazione dell'utilizzo della rete telematica, ma è consapevole che tale impegno deve essere attuato nel pieno rispetto delle previsioni normative, dei principi di necessità, pertinenza e non eccedenza dei dati sensibili e/o personali, del diritto all'oblio e dei diritti fondamentali della persona.
  In particolare, saranno allo studio ed in via di sperimentazione forme adeguate di selezione dei dati pubblicati sul sito web che evitino, per quanto possibile, che i comuni motori di ricerca esterni possano, in qualsiasi momento, in modo massivo e indiscriminato, reperire un insieme di dati sensibili e personali resi disponibili in rete.
  Sarà pertanto cura di ogni singolo Dirigente di Settore individuare, volta per volta, i casi in cui è necessario o opportuno che documenti, atti, informazioni del proprio Settore, siano accessibili attraverso la pubblicazione sul sito web dell'Ente.
  In ogni caso, sarà cura del Dirigente del Settore interessato individuare il periodo temporale entro il quale si potrà, ritenuto proporzionato in rapporto alle finalità perseguite, mantenere sul sito dell'Arca Jonica documenti, atti, e/o informazioni.

- Il Direttore Generale, Titolare del Trattamento Dati, ha provveduto con propria determinazione a designare l'Amministratore precisandone le funzioni e specificandone l'ambito di attività.
  Gli estremi identificativi delle persone fisiche designate, con l'indicazione delle funzioni ad esse attribuite, è riportato in un elenco agli atti del Settore Direzione Generale – Ufficio Privacy. Con cadenza annuale sarà verificato l'operato degli amministratori di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti.
  Il Settore, Direzione Generale - Ufficio Privacy adotterà le misure necessarie a consentire un'attività di verifica dell'operato degli amministratori di sistema alla luce delle normative vigenti in merito al trattamento dei dati.

- Aggiornamento del Documento per la sicurezza
  Il presente Disciplinare Tecnico è soggetto a revisione, deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

  - modifiche all'assetto organizzativo e gestionale, in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
  - danneggiamento o attacchi al patrimonio informativo dell'Ente tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

Titolo IV
D) Vademecum sulla sicurezza

7) Minacce

7.1 Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

7.2 Minacce a cui sono sottoposte le risorse connesse in rete

Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:
all'utilizzo della LAN/Intranet (interne);
ai punti di contatto con il mondo esterno attraverso Internet (esterne);

- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

IP spoofing

L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Packet sniffing

Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

Port scanning

Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

Highjacking

Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.

Social engineering

Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

Buffer overflow

Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

Spamming

Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

Password cracking

Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

Trojan

Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

Worm

Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

Logic bomb

Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

Malware e MMC (Malicious Mobile Code)

Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

DOS (Denial of Service)

Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

DDOS (Distributed Denial of Service)

Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete.

L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti esterne a quella della rete locale LAN.

La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

7.3 Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

7.4 Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

8) Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- utilizzo di server con configurazioni di ridondanza (da implementare);
- presenza di gruppi di continuità elettrica per il server (implementato);
- attivazione di un sistema di backup centralizzato e automatizzato (da implementare);
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet (implementato);
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico e la scansione periodica dei supporti di memoria (implementato);
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate.

8.1 Regole per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale, in seguito indicato come User-id e password personale.
User-id e password iniziali sono assegnati, dall'Ufficio Privacy.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
La User-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.
La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere obbligatoriamente modificata

dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa all'Ufficio Privacy, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni tre mesi ciascun incaricato provvede a sostituire la propria password e a consegnare all'Ufficio Privacy una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; l'Ufficio Privacy provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo sei mesi di non utilizzo.
In caso di manutenzione straordinaria l'accesso dei tecnici dell'assistenza sarà regolato come già riportato al paragrafo 2.4.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili.
Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. vengono immediatamente cambiate dopo l'installazione e al primo utilizzo.
Per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere lo user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni tre mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina la sua validità dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia

8.2 Regole per la gestione di strumenti elettronici/informatici

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- le risorse sono condivisi in rete secondo le policy di sicurezza descritte nel Dominio Active Directory;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su CD e/o dischi esterni USB saranno conservate in armadio chiuso a chiave negli uffici di competenza del trattamento dei dati;
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10

minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.

- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche;
- il fax si trova in locale ad accesso controllato (Ufficio Protocollo) e l'utilizzo, consentito unicamente agli incaricati del trattamento.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio sia stato nominato responsabile al trattamento dei dati.

8.3 Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di “scaricare“ dalla rete internet ogni sorta di file, eseguibile e non. La decisione di “scaricare” può essere presa solo dal responsabile del trattamento;
- disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su “chiedi conferma” (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta elettronica al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");

- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- è compito dell'amministratore di sistema provvedere all'aggiornamento e all'installazione delle fix/patch relative al sistema operativo;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk,definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

8.4 Incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;

- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

- evitare danni diretti alle persone;
- proteggere l'informazione sensibile o proprietaria;
- evitare danni economici;
- limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procede a:

- isolare l'area contenente il sistema oggetto dell'incidente;
- isolare il sistema compromesso dalla rete;
- spegnere correttamente il sistema oggetto dell'incidente (vedi tabella).
- documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.
Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di Incident response, tenendo presente quanto sotto indicato:

- eseguire una copia bit to bit degli hard disk del sistema compromesso;
- se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
- se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Tabella - Procedure di spegnimento

Sistema operativo	Azione
UNIX/Linux	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt.
Mac	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Cliccare Special. 3. Cliccare Shutdown. 4. Una finestra indicherà che è possibile spegnere il sistema. 5. Effettuare lo shutdown.
Windows	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Effettuare lo shutdown.

Nota: *(fonte U.S. Departement of Energy)*

9) Regolamento per l'utilizzo della rete

9.1 Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

9.2 Principi generali – diritti e responsabilità

L'Ente ARCA JONICA della Provincia di Taranto promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.
Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto viene impedito con opportune autorizzazioni che l'utente possa modificarne la configurazione.
Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore.
E' pertanto inibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema previa autorizzazione del responsabile dell'ufficio Privacy.
L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

9.3 Abusi e attività vietate

E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);

- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

9.4 Attività consentite

E' consentito all'amministratore di sistema previo autorizzazione del responsabile della Privacy:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta al punto 2.5;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

9.5 Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'Ufficio Privacy - "l'amministratore di sistema" - può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al responsabile del trattamento - Ufficio Privacy - l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

9.6 Modalità di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente è obbligato a modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nell'allegato 3.

9.7 Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni.

10) Utilizzo del proxy

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e all'autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle rappresentanze sindacali unitarie. Si ricorda che il D.L.vo 196/03 (Codice in materia di protezione dei dati personali) ribadisce quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il "*... divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze*

sindacali, la lecita introduzione in azienda". D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio dei diritti del lavoratore è opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempre che la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori. Sempre tra le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali. A titolo di esempio si possono elencare:

- la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";
- la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

Le informazioni e le attività eseguite sulla rete informatica e telematica relative agli utilizzatori, sono registrate e conservate su file (registro elettronico delle attività o file di log).

Tali file possono essere soggetti ad indagini, nel rispetto di quanto sancito dal D.L.vo 30 giugno 2003, n. 196. Inoltre, il responsabile per la sicurezza può accedere ai file degli utilizzatori per proteggere l'integrità dei sistemi informatici.

11) Videosorveglianza

Nell'esercitare attività di videosorveglianza, viene rispettato il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

a) sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
b) è scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
c) sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
d) il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai le 24 ore, in alcuni casi i 7 giorni o eventuali deroghe stabilite

dal garante;

la conservazione dei dati oltre il termine previsto alla lettera d), è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie;

i dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.

Il presente Disciplinare Tecnico, redatto in due originali, è divulgato a tutti i dipendenti per il tramite di ogni Dirigente e pubblicato sul sito istituzionale dell'Ente ARCA JONICA nella sezione Privacy.

Estensori del documento:

Ufficio Privacy:

Il Responsabile
f.to Sig. Antonio Marzia

L'Amministratore di Sistema
f.to Dott. Francesco Gregorio

Multimedia System S.a.s.

Il Responsabile
f.to Sig. Michele Salvi

DIREZIONE GENERALE – UFFICIO PRIVACY

Riservato all'Ufficio Privacy e Sicurezza **D.T._MOD./01**

Riferimento richiesta intervento n.: _____/UPS

Data: _____

RICHIESTA DI ASSISTENZA TECNICA

Prot. Servizio N. _____ /Direz. _____ Taranto, _____

== parte da compilare a cura del richiedente e fare pervenire all'UFFICIO PRIVACY ==

Descrizione elemento: ☐ Computer - ☐ Monitor - ☐ Stampante - ☐ Software - ☐ Altro

Marca e modello: _____

N.matricola /Serial number : _____

-- Ubicazione attrezzatura --

Ufficio/Struttura: ……..… Piano e stanza: ……

Utente riferimento: ……..…… Numero di telefono: ……

Descrizione dettagliata tipo di guasto/anomalia:

Data e Firma del Responsabile del Settore richiedente:

_____ _____

== Parte da compilare a cura dell'UFFICIO PRIVACY e far pervenire a MULTIMEDIA SYSTEM ==

Data presa in carico richiesta: _____ Identificativo chiamata: _____

Dotazione in: ☐ Garanzia ☐ Contratto manutenzione ☐ Altro

Note:_____

Data e Firma del Responsabile:

_____ _____

== parte da compilare a cura di MULTIMEDIA SYSTEM e fare pervenire all'UFFICIO PRIVACY ==

Descrizione dettagliata intervento: ☐ Riparazione ☐ Sostituzione ☐ Altro

Data e Firma del Responsabile:

_____ _____

RIHIESTA DI ACQUISTO

Prot. Gen. N. ……../*DIREZ.GEN./Uff.Privacy* **Taranto, ……..……**

== UFFICIO PRIVACY A UFFICIO ECONOMATO ==

Descrizione dell'acquisto: ☐ Computer - ☐ Monitor - ☐ Stampante - ☐ Software - ☐ Altro

Descrizione dettagliata specifiche tecniche:

Visto: Il Direttore Generale
Avv. Mauro Leone

Il Responsabile
Ufficio Privacy e Sicurezza
Sig. Antonio Marzia

N.B. dell'esito della presente chiamata deve essere redatto dal tecnico del fornitore, se coinvolto, un rapporto d'intervento anche quando questa resta aperta. I rapporti d'intervento vistati dall'utente dovranno essere restituiti a stretto giro all'Ufficio Privacy e Sicurezza Informatica.

Tutti i dati personali trasmessi con la presente richiesta di assistenza tecnica, ai sensi dell'art. 11, comma l, del decreto legislativo 30 giugno 2003, n. 196, saranno trattati esclusivamente per le finalità di gestione della presente richiesta e delle attività connesse alla gestione del servizio di assistenza.
Il conferimento di tali dati è obbligatorio ai fini della gestione della richiesta di assistenza tecnica. Le informazioni così acquisite potranno essere comunicate all'Ufficio Economato per eventuali necessità di acquisti, per le attività inerenti il servizio di assistenza tecnica e secondo le finalità istituzionali dell'ARCA JONICA della Provincia di Taranto.

DIREZIONE GENERALE – UFFICIO PRIVACY

Riservato all'Ufficio Privacy e Sicurezza	**D.T._MOD./02**
Riferimento richiesta intervento: n._____/UPS	
Data: ……	

Prot. Gen. N. ……/*DIREZ.GEN./Uff.Privacy*

Taranto, ……..……

Via Pitagora 144 - Tel. 099.4539411 - Fax 099.4535992

Al Responsabile dell'Uff. Privacy
e, p.c. Al dipendente/collaboratore (assente)
Sede

OGGETTO: **Istanza di accesso alla casella di posta elettronica della postazione client del dipendente assente.**

Il sottoscritto Dirigente della Direzione …… poiché:

Il collaboratore *(nome e cognome)*…… matricola n. ..... è assente;

- vi sono improrogabili esigenze di assicurare la continuità dell'attività lavorativa di seguito descritte con la necessità assoluta di prendere visione ed estrapolare i messaggi di posta elettronica in arrivo sulla casella di posta …….... assegnata al collaboratore assente,

CHIEDE

- come indicato nel "Disciplinare Tecnico", che venga effettuato all'accesso alla casella di posta elettronica sopra indicata dall'amministratore di sistema di codesta struttura o dal referente informatico esterno, per estrapolare i messaggi necessari.

Taranto, …….

Il Dirigente del Servizio

DIREZIONE GENERALE – UFFICIO PRIVACY

Riservato all'Ufficio Privacy e Sicurezza	**D.T._MOD./03**
Riferimento richiesta intervento: n._____/UPS	
Data: ……	

Prot. Gen. N. ……/*DIREZ.GEN./Uff.Privacy*

Taranto, ……..…….

Via Pitagora 144 - Tel. 099.4539411 - Fax 099.4535992

Al Responsabile dell'Uff. Privacy
e, p.c. Al dipendente/collaboratore (assente)
Sede

OGGETTO: **Istanza di accesso ai contenuti (file/cartella), della postazione client del dipendente assente.**

Il sottoscritto Dirigente della Direzione …… poiché:

il collaboratore *(nome e cognome)* …… matricola n. …… è assente;

- vi sono improrogabili esigenze di assicurare la continuità dell'attività lavorativa di seguito descritte

……

……

- è assolutamente necessario visionare ed estrapolare il file/cartella di seguito specificato, presente nella postazione client dell'utente assente

(nome file o cartella)…….....

CHIEDE

- come indicato nel "Disciplinare Tecnico", che venga effettuato l'accesso alla postazione client, dall'amministratore di sistema di codesta struttura o dal referente informatico esterno, per estrapolare il file/la cartella indicato/a.

Taranto, …….

Il Dirigente del Servizio

DIREZIONE GENERALE – UFFICIO PRIVACY

Riservato all'Ufficio Privacy e Sicurezza	**D.T._MOD/04**
Riferimento richiesta intervento: n._____/UPS	
Data: ……	

Prot. Gen. N. ……/*DIREZ.GEN./Uff.Privacy*

Taranto, ……..……

Via Pitagora 144 - Tel. 099.4539411 - Fax 099.4535992

Al Responsabile dell'Uff. Privacy
e, p.c. Al dipendente/collaboratore (assente)
Sede

OGGETTO: Verbale di accesso ai messaggi della casella di posta elettronica da parte dell'amministratore di sistema o del referente informatico esterno.

Il sottoscritto …… amministratore di sistema dell'Ente/referente informatico esterno,

DICHIARA

- Che ha effettuato l'accesso alla casella di posta elettronica della postazione client del dipendente Sig. …… in data …./…./…….. alle ore …….;
- Che, come da istanza Prot. N. …….. del …./…./…….. ha preso visione e/o inoltrato all'indirizzo di posta elettronica ……. i messaggi di posta presenti nella casella dell'utente assente Sig. ……., così come indicati nella citata istanza del Dirigente del Servizio …… e allo stesso trasferiti;
- Che non sono stati aperti i messaggi di posta elettronica il cui contenuto, così come presumibile dalle informazioni presenti nell'oggetto dei messaggi, non fosse riferibile alle esigenze di assicurare continuità all'attività lavorativa, così come specificate nell'istanza sopra indicata.

Taranto, …….

L'Amministratore di Sistema/
Il referente informatico esterno

Per asserzione il richiedente,
Dirigente

DIREZIONE GENERALE – UFFICIO PRIVACY

Riservato all'Ufficio Privacy e Sicurezza	**D.T._MOD./05**
Riferimento richiesta intervento: n._____/UPS	
Data: ……	

Prot. Gen. N. ……/*DIREZ.GEN./Uff.Privacy*

Taranto, ……

Via Pitagora 144 - Tel. 099.4539411 - Fax 099.4535992

Al Responsabile dell'Uff. Privacy
e, p.c. Al dipendente/collaboratore (assente)
Sede

OGGETTO: Verbale di accesso al/alla file/cartella da parte dell'amministratore di sistema o del referente informatico esterno.

Il sottoscritto …… amministratore di sistema dell'Ente /referente informatico esterno,

DICHIARA

- Che ha effettuato l'accesso al file/cartella della postazione client del dipendente Sig. …… in data …./…./…….. alle ore …….;
- Che, come da istanza Prot. N. …….. del …./…./…….. ha preso visione /estrapolato i seguenti dati (denominazione file/cartella) ……., presenti nel PC client del dipendente assente Sig. ……., così come indicati nella citata istanza del Dirigente del Servizio …… e allo stesso trasferiti;
- Che non sono stati aperti file o cartelle il cui contenuto, così come presumibile dalle informazioni presenti nelle proprietà, non fosse riferibile alle esigenze di assicurare continuità all'attività lavorativa, così come specificate nell'istanza sopra indicata.

Taranto, …….

L'Amministratore di Sistema/
Il referente informatico esterno

Per asserzione il richiedente,
Dirigente