POLITECNICO
MILANO 1863

Gestione dispositivi mobili

Indice

1 INTRODUZIONE 2
1.1 Premessa 2
1.2 Obiettivi del documento 3
1.3 Destinatari 3
1.4 Riferimenti normativi 3
1.5 Glossario 5
2 DISPOSITIVI PORTATILI 6
2.1 Assegnazione 6
2.2 Ritiro 7
2.3 Revoca 7
2.4 Supporto tecnico 8
2.5 Dismissione e smaltimento 8
3 MISURE MINIME DI SICUREZZA PER UN CORRETTO UTILIZZO DEI DISPOSITIVI PORTATILI 8
3.1 Utilizzo dei dispositivi mobili 8
3.2 Accesso ai dispositivi mobili 9
3.3 Connettività e navigazione da remoto 10
3.4 Supporti di memorizzazione 11
3.5 Manutenzione del dispositivo 11
3.6 Accesso in emergenza 12
4 RESPONSABILITA' E SANZIONI 12
4.1 Trasporto, perdita e furto 13
ALLEGATO 1 – Procedura ciclo di vita dei dispositivi mobili in ASICT 14

POLITECNICO
MILANO 1863

1 INTRODUZIONE

La tematica dell'utilizzo dei dispositivi portatili ha subìto nell'ultimo periodo un notevole incremento di attenzione. Motivo di questa nuova ondata di interesse si riscontra principalmente nell'aumento fortemente vertiginoso di dispositivi mobili adottati in ambito lavorativo per svolgere diverse funzioni e compiti. L'affermazione di queste tipologie di dotazioni è caratterizzata da una serie di elementi di natura tecnologica, normativa e anche sociologica che delineano dei contesti operativi significativamente innovativi e che al contempo rendono necessaria una ridefinizione degli approcci adottati per la gestione dei dispositivi portatili. Le dotazioni informatiche sono considerate strumenti di lavoro importanti e il loro utilizzo viene supportato, come già preannunciato, al fine di raggiungere determinati obiettivi. Ad oggi, con l'evoluzione digitale e l'introduzione dello smart working, l'accesso da remoto e l'utilizzo di supporti mobili è, più di prima, parte del processo produttivo e aiuta nello sviluppo del lavoro e nel mantenimento della relazione con gli utenti ma al contempo comporta un aumento dei rischi e delle minacce di natura fisica (furto, smarrimento e danneggiamento) e tecnologica (ad esempio: accessi non autorizzati, esfiltrazione di dati).

Per questi motivi, una corretta gestione e utilizzo di tali dotazioni è strettamente necessaria. Nelle presenti linee guida vengono illustrate le principali pratiche e i requisiti per una corretta gestione dei dispositivi mobili. Le linee guida in oggetto vanno a completare inoltre il *Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT*, il Modello Organizzativo Privacy e le *Istruzioni Operative per il trattamento dei dati personali* di Ateneo.

1.1 Premessa

Posto che l'utilizzo delle risorse informatiche e telematiche dell'Ateneo nonché degli altri strumenti di comunicazione messi a disposizione deve sempre ispirarsi al principio della diligenza e correttezza, il Politecnico di Milano promuove ogni opportuna misura, tanto organizzativa quanto tecnologica, volta a prevenire il rischio di utilizzi impropri di tali strumenti e delle banche dati di sua proprietà. L'introduzione di dispositivi mobili in un'organizzazione richiede infatti l'attenta elaborazione di istruzioni che tengano conto di processi, piani di formazione e il coinvolgimento della dirigenza. Pertanto, le Istruzioni Operative e le Linee Guida indicano ai possessori di dispositivi mobili, l'adozione di misure di sicurezza non solo tecniche ma anche organizzative necessarie per il corretto impiego di tali strumenti nella gestione del quotidiano nell'organizzazione. La presente linea guida, come vedremo nei paragrafi successivi, è volta in questa direzione. Agli assegnatari di dispositivi mobili è richiesto il massimo livello di consapevolezza, di attenzione e di scrupolosità nel loro impiego e nella loro custodia. Le dotazioni informatiche oggetto delle presenti linee guida permettono di costruire un legame di "vicinanza umana" oltre che di fiducia con chi si trova ad interagire con l'Amministrazione. L'utilizzo sicuro di canali e modalità diverse permette di porre la persona e la sicurezza, al centro delle attenzioni dell'organizzazione complessiva dell'Ateneo.

1.2 Obiettivi del documento

Lo scopo del documento in oggetto è di definire buone pratiche, responsabilità nei comportamenti e procedure standard da tenere in considerazione per tutti coloro che abbiano necessità di ricevere un dispositivo mobile o una qualsiasi dotazione ICT all'interno di tutta l'organizzazione dell'Ateneo. Ancorché, per coloro che necessitino di connettersi da remoto oppure di collegare supporti rimovibili portatili (ad esempio chiavette USB) a qualsiasi infrastruttura all'interno delle reti interne del Politecnico di Milano o alle relative risorse tecnologiche. Ulteriore obiettivo di questa procedura è di adeguarsi a Standard e Best Practice nazionali ed internazionali di riferimento, alle normative di legge e tutelare il patrimonio informativo da comportamenti scorretti e potenzialmente dannosi per l'immagine, la sicurezza, l'integrità e la privacy dell'Ateneo e dei suoi collaboratori, studenti, docenti e di chiunque si trovi ad interagire con l'amministrazione a qualsiasi titolo.

Si precisa che gli allegati presenti all'interno del presente documento hanno efficacia vincolante per ASICT mentre per tutte le altre strutture del Politecnico che assegnano dispositivi mobili rappresentano una *good practice* a cui ispirarsi nella gestione dei dispositivi mobili.

1.3 Destinatari

La presente linea guida è indirizzata a tutti gli utenti assegnatari di dispositivi portatili di qualsiasi tipo o che si connettano da remoto tramite l'utilizzo di questi dispositivi. Più in generale è rivolta a tutti i dipendenti, fornitori, collaboratori, consulenti, docenti e chiunque a qualsiasi titolo necessiti di una dotazione ICT nell'ambito dello svolgimento delle proprie mansioni e dei compiti agli stessi affidati dal Politecnico di Milano. Pertanto, tutti i soggetti di cui sopra sono tenuti ad osservare con la massima attenzione le misure minime di sicurezza e le norme comportamentali da tenere nell'utilizzo e nella custodia di tali dotazioni secondo le indicazioni di seguito riportate.

1.4 Riferimenti normativi

L'adozione di dispositivi mobili evoluti in ambito lavorativo ha comportato anche la necessità di adeguarsi a diversi adempimenti formali richiesti dalle leggi. Infatti, uno degli aspetti di rischio da indirizzare è dato dalla non conformità agli standard e alle best practice. Per perseguire tale obiettivo è necessario individuare in via preliminare i rimandi al contesto normativo. Di seguito i principali riferimenti normativi:

- ***Normative esterne***
  - Regolamento UE 679/2016 GDPR (General Data Protection Regulation)
  - D.lgs. 196/2003 Codice per la protezione dei dati personali "Codice privacy"
  - Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (AGiD)

- ***Regolamenti interni:***

- Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT
- Modello organizzativo privacy del Politecnico di Milano
- Istruzioni operative per il trattamento dei dati personali.

- ***Standard e best practice:***
  - UNI CEI EN ISO/IEC 27001:2017 (*Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti*)
  - NIST SP 800-24 *Guidelines for Managing the Security of Mobile Devices in the Enterprise*

1.5 Glossario

RAEE	I rifiuti di apparecchiature elettriche ed elettroniche o semplicemente rifiuti elettronici
Multi factor Authentication	L'autenticazione a più fattori è una tipologia di autenticazione elettronica in cui ad un utente X viene concesso l'accesso a un sito Web oppure ad un'applicazione solo dopo aver presentato due o più prove come ad esempio: conoscenza, possesso e inerenza.
MDM – Mobile Device Management	La gestione dei dispositivi mobili è data dall'amministrazione di dispositivi mobili, come smartphone, tablet e laptop. L'MDM viene di solito implementato con l'uso di un prodotto di terze parti che dispone di funzionalità di gestione per particolari fornitori di dispositivi mobili.
Wiping	Cancellazione definitiva/distruzione dei dati.
Root o Jailbreak	Procedure che consentono di installare, sui dispositivi a marchio Android/iOS, applicazioni e pacchetti alternativi rispetto a quelli presenti negli store ufficiali.
BYOD- Bring your own device	Termine utilizzato per identificare l'impiego di dispositivi di proprietà personale del dipendente nello svolgimento delle mansioni.
End of Life	Fine ciclo di vita di un dispositivo.

POLITECNICO
MILANO 1863

2. DISPOSITIVI PORTATILI

Come riportato all'art. 29 del Capo VI "Sicurezza e servizi ICT" del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT, per dispositivo portatile nel contesto del Politecnico di Milano vengono considerati tutti gli strumenti informatici e gli elaboratori portatili: telefoni cellulari e relative SIM, smartphone, PDA, tablet, PC e altri strumenti analoghi. Sono inclusi anche i supporti mobili di memorizzazione (memorie Flash, chiavette USB, Hard Disk Esterni, supporti ottici). Questi dispositivi, per loro natura, sono altamente vulnerabili sotto il profilo della sicurezza per i seguenti motivi:

- Esposizione al rischio di furto e di danneggiamento;
- Elevate probabilità che utenti non autorizzati accedano ai dati memorizzati;
- Posizione privilegiata di accesso esterno alle risorse del sistema.

È opportuno qualificare una procedura documentata per la gestione dell'intero ciclo di vita dei dispositivi portatili – dall'assegnazione allo smaltimento – tenendo conto di tutte le operazioni che devono essere eseguite su queste dotazioni.

Nell'ambito di questo processo il Politecnico di Milano è impegnato ad organizzare e mantenere un inventario dei dispositivi che comprenda almeno le seguenti caratteristiche minime:

- Identificazione dei dispositivi (PC, smartphone, tablet, chiavette USB…);
- Identificazione, nel caso di smartphone, della SIM;
- Lo stato del dispositivo (ad esempio: nuovo, in manutenzione, assegnato, da smaltire…);
- L'utente assegnatario del dispositivo, le modalità di assegnazione (ad esempio inserendo la data di inizio e fine assegnazione);
- Le modalità di ritiro del dispositivo portatile e di supporto tecnico;
- Una procedura di smaltimento dei dispositivi portatili.

La procedura di seguito indicata è riferita ad ASICT e viene considerata come *good practice* a cui le strutture assegnatarie dotate di loro autonomia gestionale possono adeguarsi per la gestione dei propri dispositivi mobili osservando le regole di seguito descritte.

2.1 Assegnazione

L'assegnazione dei dispositivi portatili o delle abilitazioni ICT offerte all'utenza, nel caso in cui si disponga dei requisiti per averne diritto, viene definita e approvata dalla struttura competente secondo l'articolazione delle competenze e delle funzioni previste dalla normativa di Ateneo.
La richiesta di assegnazione dovrà essere effettuata tramite compilazione di apposito form di richiesta e dovrà contenere le informazioni necessarie ad identificare la dotazione da predisporre per l'utente in base al ruolo o alla funzione ricoperta.
Esistono due modalità di assegnazione:

- Il responsabile di struttura avanza la richiesta di assegnazione della dotazione motivandola;
- Oppure, a seguito dell'attivazione di un contratto di smart working, lavoro agile o telelavoro. In questo caso c'è una procedura a parte che prevede un iter approvativo che passa dall'ufficio del personale per determinare se la dotazione può essere fornita.

Per tutte le dotazioni (apparecchi telefonici, Personal Computer, chiavette USB) l'assegnatario dovrà firmare un apposito modulo di ricevuta, che sarà predisposto e conservato dalla struttura competente dell'Amministrazione. L'assegnazione è legata al progetto del richiedente della dotazione e/o allo svolgimento di attività legate alla propria prestazione lavorativa e al proprio incarico o ad uno o più progetti specifici. In caso di cessazione del rapporto di lavoro per qualsivoglia motivo, l'assegnatario è obbligato a restituire la dotazione ricevuta. Il Politecnico di Milano si riserva inoltre la facoltà di revocare o sospendere l'assegnazione dei dispositivi portatili per mancato utilizzo, per esigenze istituzionali, per violazione delle presenti linee guida e delle altre procedure che disciplinano l'utilizzo dei dispositivi mobili, nonché per violazione della normativa in materia di tutela dei dati personali e/o delle istruzioni ricevute in qualità di autorizzato o responsabile del trattamento dei dati o di amministratore di sistema, o per eventuali fatti di reato connessi all'utilizzo di dispositivi mobili.

2.2 Ritiro

Le dotazioni informatiche sono prese in carico dall'utente presso i punti di distribuzione gestiti da ASICT. All'atto del ritiro vengono fornite all'utente assegnatario istruzioni operative per l'utilizzo e al contempo viene eseguita sul dispositivo una personalizzazione e configurazione. Inoltre, viene fatto firmare un modulo di presa consegna del PC e delle relative dotazioni (ad esempio cuffie con microfono, mouse, borsa). La restituzione dell'asset deve avvenire allo stesso punto di ritiro. Per i telefoni cellulari e relative SIM il principale punto di ritiro è presso il servizio di telefonia fissa e mobile di Ateneo previa ricezione di mail di avviso ritiro merce. Il materiale richiesto sarà consegnato solo al diretto interessato o a persona munita di delega.

2.3 Revoca

La revoca di un dispositivo mobile può avvenire a seguito di svariate circostanze come, ad esempio, in caso di cessazione del rapporto di lavoro/collaborazione, per licenziamento o qualsivoglia motivo, o qualora venga comunque revocata o non più confermata l'autorizzazione all'uso della dotazione ricevuta. In quest'ultimo caso rientrano gli accertamenti di un uso non conforme del servizio da parte dell'utente. La revoca avviene in ogni caso di violazione e/o inadempimento da parte dell'utente di quanto stabilito dal Regolamento, dalle istruzioni ricevute dall'Amministrazione e dalla normativa in materia di tutela di dati personali vigente, che sia stata accertata o relativamente alla quale sussistano gravi indizi di una condotta illecita. In caso di revoca di assegnazioni e autorizzazioni il dispositivo dovrà essere riconsegnato.

2.4 Supporto tecnico

Durante l'utilizzo dei dispositivi ricevuti in dotazione, può capitare che involontariamente si arrechi un danno o più in generale può accadere che si riscontrino dei malfunzionamenti. Pertanto, in caso di necessità di supporto tecnico sarà necessario contattare il servizio Help Desk tramite numero di telefono oppure attraverso l'apertura di ticket, per cui tutti gli utenti hanno la possibilità di segnalare guasti hardware e software.

Il supporto tecnico può essere richiesto – in modo esemplificativo e non esaustivo – per indirizzare principalmente le seguenti problematiche:

- Sostituzione in garanzia per anomalie di produzione;
- Danno accidentale;
- Installazione di software che permettono l'accesso a posta elettronica, calendario e file memorizzati in Cloud;

2.5 Dismissione e smaltimento

In caso di dismissioni gli incaricati effettuano operazioni di salvataggio e consegna al responsabile della unità organizzativa di riferimento. I dispositivi multimediali rimovibili che non sono più necessari o sono stati danneggiati devono essere riconsegnati e trattati in modo tale da evitare perdita e dispersione di dati. Il primo passaggio in caso di dismissione di dispositivo portatile è quello di effettuare operazioni di *wiping* sul dispositivo. Nel caso dei PC il ciclo di vita del dispositivo è gestito interamente all'interno del sistema di asset. A fronte della necessità di riutilizzo di supporti da parte di altri Utenti, questi possono riutilizzarli solo se i dati precedentemente contenuti non sono più intellegibili e riutilizzabili.

3 MISURE MINIME DI SICUREZZA PER UN CORRETTO UTILIZZO DEI DISPOSITIVI PORTATILI

Nell'ambito della gestione dei dispositivi mobili risulta necessario delineare delle misure minime di sicurezza per il loro utilizzo, in modo tale da evitare di incorrere in sanzioni penali o amministrative a causa di una non conformità alle principali normative ma altresì per sottrarsi ad incidenti di sicurezza che potrebbero compromettere il patrimonio informativo dell'Ateneo. Queste misure devono essere osservate – per quanto di interesse – anche dai fornitori esterni che accedano alla rete del Politecnico o che si trovino ad utilizzare dispositivi portatili nell'esercizio delle loro funzioni o nello svolgimento delle mansioni assegnate agli stessi dall'Ateneo.

3.1 Utilizzo dei dispositivi mobili

Nell'utilizzo dei dispositivi portatili (PC, tablet, smartphone, supporti di memorizzazione, chiavette USB…) è necessario osservare delle misure minime di sicurezza, in accordo con il Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT e le Istruzioni Operative per il trattamento dei dati personali di Ateneo e con il NIST 800-24. Le norme minime comportamentali per un corretto utilizzo sono riconducibili nelle seguenti:

- È necessario prestare attenzione e cura nella gestione e utilizzo dei dispositivi ricevuti in dotazione per tutelarne il corretto funzionamento;
- Il dispositivo non deve essere mai lasciato incustodito (vedi Paragrafo 4.1) così che non venga acceduto da terze parti e/o non venga smarrito;
- È vietato cedere a terzi, anche colleghi o familiari, il dispositivo assegnato dall'Ateneo;
- L'utilizzo del telefono è vincolato alla SIM ricevuta, se non diversamente autorizzato;
- È vietato il *rooting* o *jail-breaking* del dispositivo mobile;
- È vietato modificare i parametri di sistema o alterare in qualsiasi modo le misure di protezione del dispositivo (ad es. impostazioni relative alla richiesta del PIN, al blocco automatico dello schermo etc.);
- È consigliato adottare un'opportuna crittografia dei dati nel dispositivo abilitando le funzionalità già previste nei dispositivi portatili (laptop, smartphone e tablet);
- È altresì raccomandato fortemente l'aggiornamento periodico del OS e dei software del dispositivo portatile e delle applicazioni in esso installate.
- È importante assicurarsi di utilizzare dispositivi mobili (Smartphone/Tablet) con sistemi operativi non in *End Of Life.*
- Non cliccare su link o allegati in e-mail o messaggi testuali. Evitare URL o QR code sospetti o di provenienza non nota.
- La memorizzazione di informazioni di natura personale sul proprio PC oppure sulle risorse condivise (cartelle di rete e server) è vietata;
- Occorre chiudere le singole applicazioni quando gli strumenti informatici vengono lasciati accesi ed incustoditi per periodi medio-lunghi, anche quando il sistema risulta protetto da screensaver con password.

3.2 Accesso ai dispositivi mobili

Ad ogni dipendente viene assegnato un account aziendale (nominale) per accedere al sistema informativo e a tutti i servizi connessi. È responsabilità degli utenti assegnatari di account aziendale (nominale) gestire in sicurezza user-ID o componenti riservate (ad esempio, password o PIN) che permettono l'accesso agli strumenti informatici di lavoro. Gli utenti nell'utilizzo dei dispositivi ricevuti in dotazione devono proteggerne l'accesso attraverso l'impostazione di un PIN di accesso e/o altro meccanismo di sblocco *multifactor authentication* come, ad esempio, l'impronta o il riconoscimento facciale;

Nello specifico:

- La user-ID come prescritto dalla Policy AUNICA:
  - non deve essere utilizzata e condivisa con terzi;
  - la componente riservata deve essere generata secondo le regole di composizione stabilite

- La password deve rispettare i seguenti criteri descritti all'interno della Policy AUNICA:
  - essere lunga almeno 8 caratteri alfanumerici;
  - contenere almeno 2 caratteri numerici;

  - contenere almeno 2 caratteri alfabetici;
  - contenere almeno 1 carattere alfabetico maiuscolo;
  - differire dalla password precedente di almeno 4 caratteri;
  - differire dalle ultime 10 password utilizzate;
  - differire da una password usata negli ultimi 13 mesi;
- è segreta e deve essere custodita con cura, evitando di scriverla e/o memorizzarla su supporti cartacei, magnetici e/o elettronici non protetti e, in qualsiasi caso, di comunicarla a terzi;
- deve essere gestita secondo procedure che prevedano almeno che gli utenti:
  - se si tratta del PIN, provvedano alla modifica al primo accesso;
  - se si tratta della password, cambino quella assegnata per accedere ad un servizio al primo accesso e a seguito di eventuali ripristini, in particolar modo in caso di sospetto o avvenuta violazione della sua riservatezza, avendo cura di non scegliere le due precedenti password utilizzate.
  - si accertino di non essere osservati nella digitazione;
  - nel caso di sospetto o avvenuta violazione delle credenziali Aunica deve essere inviata apposita notifica alla struttura competente in modo da essere modificata tempestivamente (se consentito dal dispositivo utilizzato)

3.3 Connettività e navigazione da remoto

La rete telematica e i servizi ICT del Politecnico di Milano rappresentano un bene comune e condiviso dell'Ateneo; in quanto strumenti di lavoro e di promozione delle attività accademiche, di ricerca, di didattica, di terza missione e di logistica infrastrutturale sono soggetti a restrizioni d'uso qualora siano verificate infrazioni che possano comprometterne il funzionamento o il rispetto delle normative di legge. Nello specifico:

- L'utilizzo personale della rete, ove non espressamente vietato deve comunque essere guidato dalla lealtà e dalla moderazione;
- È vietato condividere la connessione dati del dispositivo mobile con altri utenti o con dispositivi non aziendali se non per giustificati motivi di servizio;
- È sconsigliato utilizzare reti Wi-Fi pubbliche non autenticate e non cifrate. Qualora fosse necessario utilizzare reti pubbliche è comunque consigliato utilizzare la VPN fornita dal servizio ASICT;
- Gli utenti assegnatari non devono installare applicazioni o app da store non ufficiali o da link e/o portali web non sicuri.

In conformità con quanto previsto dal Regolamento d'Ateneo ASICT e dalle Istruzioni operative di Ateneo si riserva la possibilità di scollegare, inibire l'accesso o disattivare qualunque dispositivo di rete non autorizzato o che effettui tentativi di compromissione alle funzionalità degli strumenti o all'immagine di Ateneo.
In aderenza alle previsioni delle Istruzioni Operative di Ateneo, ("UTILIZZO DELLA RETE INTERNET" - pagina 90) l'Ateneo si riserva, a tutela del patrimonio informativo, di ridurre al minimo i rischi derivanti dall'uso improprio della rete dati e della navigazione in Internet. L'Amministrazione può adottare idonee misure

tecniche volte a ridurre navigazioni a siti non correlati all'attività lavorativa e a prevenire eventuali condotte illecite e/o fatti di reato. Al tal fine garantire la sicurezza dei dati e l'ottimale funzionamento del sistema, a salvaguardia del patrimonio dell'Ateneo, potrà avvalersi di opportuni hardware e software automatici (antivirus, antispam, filtraggio dei contenuti) con l'implementazione di opportune Block List. L'utilizzo degli strumenti informatici di Ateneo per lo svolgimento delle attività lavorative in modalità remota (es. telelavoro o Smart working) prevedono le stesse misure di protezione infrastrutturali in essere durante le attività svolte in presenza, ad es. la connessione in VPN alla rete di Ateneo beneficia degli stessi controlli in termini di filtraggio di quando connessi in presenza dalla sede.

È competenza di ARUO richiedere di limitare o inibire l'accesso a internet per uso personale della rete di Ateneo verso determinate categorie di siti web non pertinenti con l'attività lavorativa e/o di limitare l'accesso a internet in determinate fasce orarie.

3.4 Supporti di memorizzazione

I supporti di memorizzazione portatili (chiavette usb, ecc) rappresentano un veicolo per infezioni virali e ~~per~~ possono rappresentare un rischio ~~i reati contro~~ alla riservatezza delle informazioni e la sicurezza dei sistemi. Pertanto, l'utilizzo di questi supporti deve essere limitato allo scambio di file aventi natura lavorativa e solo nelle ipotesi in cui non sia possibile utilizzare mezzi alternativi come la posta elettronica, le cartelle di rete condivise, o il file transfer diretto. In linea generale:

- Non è consentito scaricare file contenuti in supporti magnetici/ottici per finalità diverse da quelle lavorative e ad ogni modo mai al di fuori delle ipotesi consentite.
- È strettamente necessario eseguire backup e ripristino delle informazioni nel caso dei PC portatili;
- Il backup dei dati presenti sul dispositivo deve essere effettuato esclusivamente su postazioni di lavoro aziendali o in spazi di archiviazione predisposti;
- Se i supporti di memorizzazione sono impiegati per il trattamento di dati sensibili o giudiziari il loro utilizzo è strettamente limitato alle ipotesi e ai soggetti autorizzati;
- Il riutilizzo è invece ammesso solo dopo cancellazione sicura dei dati da parte del personale incaricato dalla struttura di appartenenza, in conformità al Provvedimento a carattere generale dell'Autorità garante per la protezione dei dati personali del 13 ottobre 2018 (Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali).

3.5 Manutenzione del dispositivo

Bisogna evitare di intervenire direttamente sugli strumenti informatici in dotazione richiedendo l'opportuno supporto tecnico dell'Amministrazione. In particolare, la manutenzione o la riparazione di dispositivi aziendali deve essere eseguita solo da personale espressamente autorizzato dall'Ateneo; è severamente vietato utilizzare servizi di riparazione esterni. L'utente è tenuto a contattare il personale preposto della struttura di appartenenza per la risoluzione di guasti o malfunzionamenti o per l'eventuale sostituzione del

dispositivo. Evitare di rimuovere, modificare o installare componenti hardware degli strumenti informatici in dotazione se non preventivamente autorizzati e riferire prontamente un eventuale perdita, furto, danneggiamento o malfunzionamento degli strumenti informatici alle competenti funzioni aziendali secondo la normativa e le procedure in uso.

3.6 Accesso in emergenza

Le misure di sicurezza per un corretto utilizzo dei dispositivi portatili, elencate nelle presenti linee guida potranno subire deroghe, ove fosse necessario a chi deve operare per sbloccare un servizio essenziale. Queste deroghe dovranno essere approvate dall'ufficio competente. Possono considerarsi casi di emergenza ad esempio le seguenti situazioni:

- Un'interruzione generale dei servizi di rete o di singoli plessi;
- Un'interruzione generale della fonia;
- L'interruzione generalizzata dei servizi di posta elettronica;
- Un'interruzione dei servizi di virtualizzazione delle aule durante l'erogazione di un servizio (lezione/esame/corso ecc.), ove il servizio risulti compromesso;
- L'interruzione di un servizio informatico durante eventi istituzionali e cerimonie di notevole rilevanza per l'Ateneo;
- L'interruzione di un servizio informatico in concomitanza a scadenze di adempimenti istituzionali inderogabili e indifferibili (immatricolazioni/bandi ecc.);

Non sono invece da considerarsi emergenze tutte quelle situazioni in cui l'incidente informatico è circoscritto a singole postazioni o a un malfunzionamento di singolo pc, smartphone, chiavetta USB, malfunzionamento della rete di un singolo ufficio o di attrezzature all'interno delle aule didattiche.

Inoltre, qualora, nell'accesso in emergenza si utilizzino credenziali/utenze tecniche di massimi privilegi è vietato salvare le stesse in chiaro sui dispositivi portatili aziendali e/o privati.

È sempre e comunque responsabilità di tutti i destinatari delle presenti linee guida osservare le regole prescritte dalla stessa, anche nei casi in cui si trovino impossibilitati ad utilizzare le dotazioni informatiche fornite dall'Amministrazione e debbano pertanto utilizzare strumenti di proprietà personale o di terzi. Sarà loro cura sincerarsi che gli strumenti in uso siano sicuri, conformi alle linee guida e non mettano in alcun modo a repentaglio la sicurezza e il patrimonio informativo dell'Ateneo.

4 RESPONSABILITA' E SANZIONI

L'utente assegnatario di un dispositivo mobile è ritenuto responsabile degli strumenti informatici a lui assegnati, che non deve cedere o prestare a terzi, delle credenziali di accesso messi a sua disposizione e dei dati contenuti. Si tiene a ribadire che i dispositivi mobili assegnati sono comunque di proprietà dell'Ateneo e sono finalizzati a rendere agli utenti più agevole la prestazione lavorativa o i compiti affidati. L'utilizzo per scopi personali è ammesso solo nei limiti di un ragionevole utilizzo e comunque per finalità che non vadano

contro all'ordine pubblico, all'etica e alla legge o in modi che possano compromettere il corretto funzionamento dei dispositivi o arrecare pregiudizio o danno di immagine all'Amministrazione.

Come previsto dall'art. 25 del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT e dalle Istruzioni Operative, il Politecnico di Milano si riserva di verificare che venga fatto un corretto utilizzo degli strumenti di lavoro, impegnandosi ad esercitare tale prerogativa nel rispetto della libertà e della dignità dei lavoratori.

Nel caso in cui riscontri violazioni accertate delle regole stabilite nel Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT, dalle Istruzioni Operative e dalla presente linea guida, al fine di evitare ripercussioni sulla rete, sui servizi, sulle postazioni di lavoro e sui dispositivi mobili, i responsabili dei Servizi Informatici, competenti nella materia, possono disporre la disconnessione.

Si disconnetterà un host dalla rete, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria a garantire senza alcun ritardo l'integrità o il funzionamento della rete del Politecnico di Milano o per impedire un danno all'Ateneo. Nel momento in cui si accerti che l'utente ha violato ~~le~~ norme di sicurezza, la struttura competente interviene, fermo restando la segnalazione agli Organi di vertice competenti, anche al fine di avviare eventuali azioni di natura disciplinare, civile e/o penale. Infine, la struttura competente si riserva anche la facoltà di proseguire a rimuovere qualsiasi file o applicazione ritenuta dannosa per la sicurezza del sistema ovvero acquisita o installata in violazione della legge e/o delle presenti linee guida o del regolamento d'Ateneo.

4.1 Trasporto, perdita e furto

I dispositivi mobili sono spesso utilizzati al di fuori del perimetro di controllo dell'organizzazione, pertanto, la movimentazione e la custodia degli stessi dovrà essere effettuata con l'estrema consapevolezza dei rischi di sicurezza che gravano. Deve essere cura degli assegnatari dei dispositivi mobili trasportare gli strumenti informatici di lavoro in modo adeguato e avendo cura di non lasciarli mai incustoditi in luoghi pubblici o non adeguatamente protetti; in particolare nel caso di viaggi di lavoro gli utenti devono:

- tenerli sempre con sé;
- evitare di lasciarli incustoditi in automobile (anche se chiusa a chiave);
- in albergo riporli, ove possibile, in casseforti o simili.

In caso di furto o smarrimento è sempre necessario presentare denuncia ed esibirne copia all'ufficio competente che provvederà a sostituirne con uno identico o di pari categoria.

POLITECNICO
MILANO 1863

ALLEGATO 1 – Procedura ciclo di vita dei dispositivi mobili in ASICT

Assegnazione

PC portatili

La struttura a cui far riferimento per l'assegnazione dei PC e delle dotazioni ad esso correlate è il DESKTOP AS A SERVICE, PERSONAL AND TEAM PRODUCTIVITY TOOLS – UDAS. Esistono sono due modalità di assegnazione:

- Il responsabile di struttura avanza la richiesta di assegnazione di PC motivandola;
- A seguito dell'attivazione di un contratto di smart working, lavoro agile o telelavoro. In questo caso c'è una procedura che prevede un iter approvativo che passa dall'ufficio del personale e una volta che quest'ultimo approva la dotazione chiede ad ASICT di fornire il dispositivo mobile.

Telefoni cellulari, Tablet e SIM

La struttura a cui far riferimento per l'assegnazione di Telefoni cellulari e SIM è ADMINISTRATION SERVICES – UADM. In questo caso l'assegnazione avviene tramite apertura di ticket da parte del responsabile che fa richiesta di tale dotazione.

Ritiro

PC Portatili

Il punto di ritiro dei personal computer è il service desk del Polimi. All'atto del ritiro vengono fornite all'utente assegnatario istruzioni operative per l'utilizzo e al contempo viene eseguita sul dispositivo una personalizzazione e configurazione. Inoltre, viene fatto firmare un modulo di presa consegna del PC e delle relative dotazioni (ad esempio cuffie con microfono, mouse, borsa). La restituzione dell'asset deve avvenire allo stesso punto di ritiro.

Telefoni cellulari, Tablet e SIM

Per i telefoni cellulari e relative SIM il principale punto di ritiro è presso il servizio di telefonia fissa e mobile di Ateneo previa ricezione di mail di avviso ritiro merce. Il materiale richiesto sarà consegnato solo al diretto interessato o a persona munita di delega. Al contrario dei PC non c'è un apposito modulo di consegna da far firmare, in quanto come detto in precedenza, avviene tramite apertura di ticket dal responsabile del servizio. Al momento del ritiro, vengono comunque fornite le indicazioni necessarie per l'utilizzo e la custodia del telefono cellulare e della SIM.

Supporto Tecnico

PC portatili

In caso di guasti o malfunzionamenti, il servizio a cui far riferimento è il DESKTOP AS A SERVICE, PERSONAL AND TEAM PRODUCTIVITY TOOLS – UDAS Il Service Desk risponde sia tramite telefono oppure tramite

l'apertura di ticket di supporto, per cui tutti gli utenti hanno la possibilità di segnalare guasti hardware e software. Al momento della segnalazione c'è una prima istruttoria svolta da un operatore di primo livello per indirizzare la problematica. Se è un problema software dove possibile si agisce da remoto, se invece la problematica è hardware si chiede all'utente assegnatario di riconsegnare il dispositivo e ne viene dato uno in sostituzione. Sul dispositivo guasto vengono fatte le valutazioni necessarie e viene deciso se spedirlo in garanzia oppure – nel caso sia a fine vita – si ha la sostituzione del dispositivo.

Telefoni cellulari, Tablet e SIM

In caso di necessità di supporto tecnico è necessario aprire un apposito ticket di guasto al servizio di ADMINISTRATION SERVICES – UADM che si occupa, tra le altre cose, proprio della gestione dei ticket di richiesta d'assistenza/intervento assegnati dal sistema integrato di Help Desk o, eventualmente, pervenuti mediante altri canali. Normalmente, si richiede di portare il dispositivo alle condizioni di fabbrica per poter provvedere al supporto tecnico.

Dismissione e smaltimento

PC portatili

Il primo passaggio in caso di dismissione di un PC è quello di effettuare operazioni di wiping sul dispositivo, successivamente viene dato in gestione all'AREA GESTIONE INFRASTRUTTURE E SERVIZI (AGIS)la quale ha dei contratti per la consegna di volumi di materiale RAEE**.** Nel caso dei PC il ciclo di vita del dispositivo è gestito interamente all'interno del sistema di asset, dunque nel momento in cui il dispositivo viene riconsegnato il suo "*status*" all'interno dell'asset dovrà subire una modifica. La risorsa nuovamente disponibile, viene quindi conservato nei magazzini preposti, in attesa di definirne la destinazione d'uso e potrà essere riassegnato oppure destinato allo smaltimento.

Telefoni cellulari, Tablet e SIM

In questi casi non è il Politecnico di Milano che effettua la dismissione e smaltimento in quanto le dotazioni non sono di proprietà ma a noleggio e dunque vengono restituiti al gestore della convenzione che è di volta in volta attiva. Non viene al contempo effettuato un aggiornamento dell'asset inventory ma vi è un'apposita applicazione per censire sia cellulari che SIM.

Responsabilità e sanzioni

PC portatili

Il PC e i programmi con cui è equipaggiato sono affidati a ogni singolo utente come strumenti di lavoro e pertanto sono da custodire in modo appropriato. Deve essere prontamente segnalato all'Area DESKTOP AS A SERVICE, PERSONAL AND TEAM PRODUCTIVITY TOOLS - UDAS , il danneggiamento o lo smarrimento di tali strumenti. In caso di furto è necessario presentare regolare denuncia alle autorità competenti entro ventiquattro ore e consegnarne copia ad ASICT, così che possano essere intraprese azioni volte alla garanzia della riservatezza delle informazioni.

POLITECNICO
MILANO 1863

Telefoni cellulari,Tablet e SIM

Per quanto riguarda la parte di telefonia mobile, in caso di furto o smarrimento è necessario presentare denuncia e solo in quel caso il Gestore potrà provvedere ad effettuare la sostituzione dell'apparato smarrito/rubato con uno identico o di pari categoria.