1 Scopo

Questa politica di uso accettabile definisce gli obiettivi per l'adozione di standard specifici circa l'uso professionale e appropriato degli strumenti informatici e delle informazioni che trattano. La politica è valida per tutti i dipendenti, fornitori, produttori, partner e agenti che operano per conto del Titolare del trattamento dei dati così come indentificato nelle informative redatte ai sensi degli artt. 13 e 14 GDPR, a cui, da qui in poi, verrà fatto riferimento con "incaricati".

2 Obiettivi

Le informazioni, i sistemi, i servizi e la dotazione forniti (come desktop, laptop, handheld, PDA, reti, posta elettronica, software, applicazioni, telefoni, segreterie telefoniche e fax) sono di proprietà del Titolare e forniti per raggiungere le finalità istituzionali del Titolare.
Inoltre, il Titolare acconsente, nei limiti indicati nella procedura denominata "*Politiche aziendali sull'utilizzo dei dispositivi personali nel posto di lavoro; uso, accesso privilegiato alle informazioni aziendali e loro applicazioni*" in revisione corrente, di utilizzare strumenti informatici personali (BYOD).
L'impiego di qualsiasi informazione, sistema, servizio e/o tipo di dotazione illegale, persecutoria, offensiva, dannosa o che viola il codice etico o altre politiche, standard o linee guida del Titolare costituisce una violazione a questa politica.
Il Titolare si riserva il diritto di controllare, registrare, rendere pubbliche e revisionare le proprie informazioni, sistemi, servizi e dotazioni, in ottemperanza alle leggi e ai regolamenti nazionali e comunitari vigenti. I requisiti specifici per l'uso corretto della navigazione Internet, della posta elettronica, dei sistemi di comunicazione, del software, dei servizi e dei dispositivi sono forniti di seguito.

3 Standard per l'uso accettabile degli strumenti informatici (Internet, Posta Elettronica, Sistemi di Telecomunicazione, Videoconferenze, Computer e Software)

3.1 Uso lavorativo

Gli incaricati sono responsabili delle attività eseguite sugli strumenti informatici con il proprio account.
Le risorse informatiche del Titolare devono essere impiegate per attività autorizzate dal Titolare, in ottemperanza alle leggi e ai regolamenti vigenti.
Il Titolare permette occasionalmente ai propri incaricati l'uso a scopo personale delle risorse informatiche, a condizione che:

a) non interferisca con le prestazioni lavorative dell'incaricato o di qualsiasi altro collega;
b) non abbia un impatto negativo sulle prestazioni del computer o della rete;
c) non violi altre politiche, direttive o linee guida del Titolare.

3.2 Uso improprio

Gli incaricati non devono assumere l'identità di altri incaricati, creare intestazioni false o fuorvianti nella busta del messaggio e-mail o fornire servizi di messaggistica non autorizzati.
Le risorse informatiche del Titolare NON devono essere usate per:

- attività illegali o improprie,
- operazioni che interferiscono con le normali attività del Titolare,
- attività che violano il codice etico o le politiche del Titolare,
- attività che interferiscono con le proprie prestazioni professionali o quelle di altri incaricati.

Le risorse informatiche del Titolare non devono essere usate per accedere a, trasmettere, ricevere, stampare o immagazzinare i seguenti tipi di materiale:

- messaggi persecutori, dispregiativi, discriminanti o offensivi;
- messaggi indesiderati a destinatari che non li hanno richiesti c.d. "*spamming*";

- messaggi o immagini oscene, sessualmente esplicite o a orientamento sessuale;
- invio di messaggi per scopi personali, politici o non collegati agli scopi del Titolare;
- catene di Sant'Antonio, messaggi "*joke a day*", attività sportive e scommesse, o falsi avvertimenti su virus e altro;
- umorismo, commenti o immagini che contengano diffamazione etnica, epiteti razziali o qualsiasi altra forma di comunicazione che possa offendere, disprezzare o imbarazzare gli altri in base alla razza, alla nazionalità, al colore della pelle, al genere, alle preferenze sessuali, all'età, alla disabilità, al credo politico o religioso o altro.

Le risorse informatiche del Titolare non devono essere impiegate per disabilitare o sovraccaricare deliberatamente sistemi o reti, o per eludere qualsiasi sistema atto a proteggere le informazioni del Titolare e dei suoi lavoratori.
Le risorse informatiche del Titolare non devono essere usate per sollecitare, pubblicizzare o perseguire commerci non legati all'attività del Titolare.
Le risorse informatiche del Titolare non devono essere usate per diffondere di informazioni riservate o sensibili senza autorizzazione.
Le risorse informatiche del Titolare non devono essere usate per eseguire deliberatamente operazioni che consumano o monopolizzano scorrettamente le risorse delle apparecchiature (come l'invio massivo di e.mail o di catene di Sant'Antonio, iscrizioni a gruppi chat, iscrizioni a liste e.mail estranee alle attività del Titolare, giocare e scaricare file molto pesanti – superiori a 20 MB).
Le risorse informatiche del Titolare possono essere impiegate per alcune attività speciali (come la partecipazione a gruppi chat, blog e forum) solo per condurre attività autorizzate.
Le risorse informatiche del Titolare non devono essere usate per tracciare le attività ufficiali.
Condividere le credenziali di autenticazione o le password di accesso ai sistemi informatici è severamente proibito.

3.3 Sanzioni e denuncia d'uso illecito

Le violazioni della politica d'uso delle risorse informatiche verranno documentate e possono portare alla revoca dei diritti di accesso ai sistemi e/o azioni disciplinari.
Inoltre, il Titolare si riserva il diritto di intraprendere a propria discrezione, azioni legali per danni derivanti da qualsiasi violazione.
Prima di accedere per mezzo della rete aziendale, ogni incaricato deve aver preso visione ed espressamente accettato quanto contenuto in questa politica circa l'utilizzo delle risorse informatiche.
Inoltre, gli incaricati sono tenuti a denunciare l'uso illecito (reale o sospetto) delle risorse informatiche e la ricezione di contenuti discutibili informando il Responsabile IT affinchè recepisca l'evento.
Gli incaricati devono altresì cambiare le proprie password se sospettano o hanno la certezza che qualcun altro le conosca, e sono tenuti ad avvertire immediatamente i servizi IT circa l'eventuale compromissione delle password.

4 Standard per l'uso accettabile di Internet

L'uso corretto della navigazione prevede requisiti specifici per l'impiego delle risorse Internet (come collegamenti e programmi per la navigazione – browser).

4.1 Software per la navigazione

Gli incaricati devono usare il software di navigazione e la configurazione approvati dal Titolare.
Gli incaricati non devono modificare le impostazioni di sicurezza del software di navigazione.

4.2 Download

Usando le risorse Internet del Titolare, gli incaricati si attengono alle leggi sul copyright e agli accordi di licenza per il materiale scaricato da Internet (come software, documenti, messaggi, rappresentazioni grafiche, musica o video).
Senza esplicita autorizzazione, gli incaricati non devono scaricare materiale che richieda una licenza d'uso, un abbonamento o tassa per la registrazione, o che non sia riferibile alle necessità professionali del Titolare.

Gli incaricati non devono caricare o scaricare, inviare, ricevere, immagazzinare o stampare:

- software (freeware, shareware, commerciale o di pubblico dominio),
- materiale esterno, o proveniente da persone o da aziende sconosciute.

4.3 Caricamento di materiale

Se non espressamente autorizzati, agli incaricati è fatto divieto di inviare, trasmettere o, in ogni caso, distribuire informazioni proprietarie, dati o altre informazioni confidenziali che appartengono al Titolare.
Quando autorizzati a trasferire tali informazioni, ai dipendenti viene richiesto di usare solo strumenti sicuri e autorizzati per il trasferimento.

4.4 Profili d'uso

Il Titolare ha identificato profili d'uso diversi basati sulla responsabilità del ruolo.
Di seguito i principali:

- standard,
- amministratore di sistema.

Il profilo *standard* viene assegnato a tutto il personale aziendale, a tutti i fornitori e collaboratori per l'espletamento delle proprie mansioni.
Il profilo standard permette l'accesso a siti web generici non esplicitamente bloccati, come quelli appartenenti alle categorie di seguito elencate (ma non limitate a):

- Droga
- Protezione estesa
- Scommesse, illegalità, contenuto discutibile
- Intolleranza
- Militanza ed estremismo
- Domini "in parcheggio"
- Sicurezza
- Gusto opinabile
- Violenza

Mentre, invece, il profilo standard non permette l'accesso a siti web specifici esplicitamente bloccati, come quelli appartenenti alle categorie di seguito elencate:

- Materiale per adulti

4.5 Procedura di autorizzazione

Quasiasi modifica alle regole di profilazione o assegnazione all'utente, se non esplicitamente proibite dai regolamenti, può essere richiesta al reparto IT.

5 Standard d'uso accettabile della posta elettronica

Questo standard per l'uso accettabile della posta elettronica fornisce requisiti specifici circa l'uso corretto e appropriato delle risorse di posta elettronica (come programmi per leggere e inviare le e.mail e server di posta elettronica).

5.1 Best practices

Obblighi degli incaricati:

1. mantenere la cartella "Posta in arrivo" più pulita possibile; organizzare i messaggi in cartelle;
2. cancellare i messaggi non più necessari;
3. comprimere gli allegati voluminosi per risparmiare banda e risorse di sistema;
4. nel caso di un alto numero di destinatari, valutare l'impiego del campo CCN (copia di conoscenza nascosta), al fine di garantire la privacy dei destinatari;

5. se si dovessero ricevere messaggi (via e-mail o intranet) offensivi, spiacevoli, persecutori o intimidatori, bisogna informare immediatamente il proprio responsabile. È importante "tracciare" il più velocemente possibile tali messaggi;
6. non aprire allegati e-mail o selezionare collegamenti web nel corpo del messaggio se non si considera attendibile il mittente;
7. chiuso il programma per la posta elettronica, attendere qualche secondo prima di spegnere il PC.

5.2 Programmi per la posta elettronica

Gli incaricati devono usare il programma di posta elettronica nella versione e con la configurazione approvati dal Titolare.
Gli incaricati non devono regolare le impostazioni email per essere meno restrittive rispetto alle configurazioni approvate dal Titolare.
Gli incaricati non devono usare funzioni o programmi che inoltrano automaticamente la posta, a meno che non vengano autorizzati.
Gli incaricati non devono usare funzioni o programmi che oscurano o mascherano l'identità del mittente.

5.3 Materiale scaricato

Usando le risorse Internet del Titolare, gli incaricati si devono attenere alle leggi sul copyright e agli accordi di licenza per il materiale scaricato da Internet (come software, documenti, messaggi, rappresentazioni grafiche, musica o video).
Gli incaricati non devono scaricare materiale che richieda una licenza d'uso, un abbonamento o tassa per la registrazione, o che non sia riferibile alle necessità professionali del Titolare, senza esplicita autorizzazione.
Senza autorizzazione, gli incaricati non devono caricare, scaricare, inviare, ricevere, immagazzinare o stampare i seguenti materiali:

- Software (freeware, shareware, commerciale o di pubblico dominio)
- Materiale esterno, o proveniente da persone o da aziende sconosciute agli incaricati.

5.4 Spazio e restrizioni tecniche

Sono state impostate alcune restrizioni tecniche per garantire la salute ed evitare lo spreco di risorse del sistema di posta elettronica

5.5 Protezione delle informazioni sensibili, riservate e a uso interno

Le informazioni sono un bene prezioso per il Titolare, quindi devono essere opportunamente protette.
Le attività strategiche del Titolare "*core*" richiedono la gestione di:

- **dati personali**: vengono gestiti dati personali degli interessati.
- **altre informazioni interne o confidenziali**: comunicazioni interne, informazioni finanziarie, contratti commerciali e/o di terze parti, piani interni e in generale ogni tipo di informazione aziendale e/o commerciale riservata o documenti con un'indicazione interna specifica che identifica il contenuto come confidenziale.

Gli incaricati che necessitano di inviare, ricevere o, in generale, distribuire informazioni proprietarie, dati o altre informazioni confidenziali appartenenti al Titolare, devono assicurarsi che i dati vengano inviati attraverso il sistema di sicurezza della posta elettronica approvata dal Titolare.

5.6 Conseguenze delle violazioni

Le violazioni della politica d'uso della posta elettronica verranno documentate e possono portare alla revoca dei diritti di accesso ai sistemi e/o azioni disciplinari.
Inoltre, il Titolare si riservano il diritto di intraprendere, a propria discrezione, azioni legali per danni derivanti da qualsiasi violazione. Al Titolare potrebbe anche essere richiesto dalla legge di informare le autorità competenti circa determinate attività illegali.

6 Standard d'uso accettabile dei sistemi di telecomunicazione

L'uso corretto dei sistemi di comunicazione prevede requisiti specifici per l'impiego corretto e appropriato di risorse come telefoni, cellulari, fax e segreterie telefoniche.

6.1 Sistema telefonico

L'uso di chiamate *long distance* e l'impiego di funzioni di conferenza è destinato solo a scopi lavorativi.
Gli incaricati devono prendere precauzioni quando discutono di informazioni proprietarie o riservate in ambienti dove potrebbero essere sentite da terze parti non autorizzate.
Se, per qualsiasi ragione, occorre lasciare la chiamata, si raccomanda di metterla in modalità attesa, in modo che non possano essere sentite altre informazioni potenzialmente confidenziali che si stanno discutendo nell'ufficio.

6.2 Segreteria telefonica

Gli incaricati non devono inoltrare chiamate oltre il confine del Sistema telefonico interno.
Gli incaricati non devono lasciare messaggi che contengono informazioni confidenziali o proprietarie nella segreteria telefonica, dal momento che potrebbero essere ascoltati da altre persone non autorizzate.

6.3 Stampanti, fotocopiatrici e fax

Le stampanti, le fotocopiatrici e i fax devono essere liberi da carte quando non vengono usati.
Per evitare di stampare accidentalmente su un dispositivo di rete, gli incaricati si devono assicurare che la stampante predefinita sia quella corretta.
È responsabilità della persona che stampa raccogliere i propri documenti.

7 Standard d'uso accettabile della videoconferenza

Questa politica di uso accettabile definisce gli obiettivi per l'adozione di standard specifici circa l'uso professionale e appropriato dei sistemi di videoconferenza del Titolare.

7.1 Sicurezza del sistema di videoconferenza

Il Sistema di videoconferenza del Titolare permette al personale di organizzare conferenze con altri incaricati interni all'Azienda o con partner esterni. Il Titolare incoraggia l'impiego delle videoconferenze, dal momento che è un modo di lavorare rispettoso per l'ambiente e che permette di risparmiare tempo e denaro.
In ogni caso, i sistemi di videoconferenza, come ogni servizio IT, hanno le proprie vulnerabilità e rischi associati per la sicurezza.
Per un uso sicuro del sistema di videoconferenza, occorre attenersi allo specifico Regolamento integrato dalle seguenti raccomandazioni di ordine generale:

1. gli incaricati devono usare solo il sistema di videoconferenza indicato dal Titolare. Il Titolare NON autorizza l'uso di altri sistemi (come, ad esempio, MSN, Skype - versione consumer - o Google HangOut);
2. assicurarsi che le videocamere non siano posizionate dove possano inavvertitamente riprendere documenti sensibili, schermi di computer sulle scrivanie intorno o che i microfoni non raccolgano conversazioni private che avvengono nei dintorni;
3. le videocamere e i microfoni devono essere spenti quando non vengono usati, scollegando l'alimentazione, i cavi di collegamento o usando tappi per obiettivi;
4. quando si devono discutere informazioni sensibili con organizzazioni esterne, assicurarsi dell'identità degli interlocutori prima di stabilire una videoconferenza. Si tenga presente che le videoconferenze potrebbero essere registrate e riprodotte in seguito.

8 Standard per l'uso accettabile dei computer e dei software

Questa politica di uso accettabile definisce gli obiettivi per l'adozione di standard specifici circa l'uso professionale e appropriato dei computer e dei software (come laptop, workstation, dispositivi portatili e strumenti software per la produttività) sia di proprietà del Titolare, sia BYOD.

8.1 Custodia della dotazione

L'equipaggiamento in funzione che non è bloccato non dovrebbe mai essere incustodito.
La sessione dell'utente non deve essere collegata quando il computer o il laptop non è custodito. Quando l'utente per qualsiasi ragione si deve spostare dal proprio posto di lavoro, deve bloccare il computer. L'accesso al computer/laptop deve essere protetto da password, come da politica di gestione delle password.
Per evitare il furto, i dispositivi che vengono lasciati incustoditi in aree pubbliche devono essere protetti fisicamente con key-lock o equivalenti.

8.2 Uso illecito

Gli incaricati sono tenuti a denunciare l'uso illecito (reale o sospetto) dei computer o dei software del Titolare ovvero dei sistemi BYOD e la ricezione di contenuti discutibili informando il Responsabile IT.
Gli incaricati devono cambiare le password del computer e/o dei software se sospettano o scoprono che qualcun altro le conosca.
Gli incaricati devono avvertire immediatamente i servizi IT del Titolare circa l'eventuale compromissione delle proprie password.

9 Supporti di memorizzazione portatili (supporti rimuovibili)

L'uso di supporti di memorizzazione portatili, come CD/DVD, dischi rimuovibili, schede di memoria, dischi USB eccetera in linea generale non è permesso.
Se bisogna registrare informazioni o dati personali su supporti portatili (estrema *ratio*), gli incaricati devono eseguirne il backup. Tutti gli incaricati che utilizzano dispositivi portatili, come laptop, PDA, smartphone e chiavette USB, devono assicurarsi che i dati non vengano registrati in modo permanente su tali supporti e devono trasferirli negli archivi del Titolare.

9.1 Uso lavorativo

Si dovrebbero impiegare solo i supporti di memorizzazione rimuovibili forniti dagli Titolare e dovrebbero essere "*chiusi*" e rimossi quando non più in uso.
Se si devono trasferire informazioni riservate su supporti rimuovibili, assicurarsi che vengano gestite in modo sicuro e non vengano lasciate su quel supporto a tempo indeterminato. La posizione più sicura per le informazioni e per i dati personali è negli archivi del Titolare. Se necessario trasferire dati su supporti rimuovibili, il supporto deve essere criptato con software di sicurezza appropriati.

9.2 Uso illecito

Gli incaricati non devono usare i supporti di memorizzazione rimuovibili forniti dal Titolare per immagazzinare dati o file estranei all'attività del Titolare, come immagini, file multimediali (come MP3, film eccetera) o materiali soggetto a copyright che non appartiene al Titolare.

9.3 Smaltimento sicuro

I supporti che non sono più necessari devono essere smaltiti in modo sicuro. I supporti che contengono informazioni riservate, sensibili o che permettano di identificare le persone devono essere distrutti in modo sicuro.

9.4 Protezione fisica

Per garantire la sicurezza delle informazioni sui dispositivi rimuovibili, alla fine della giornata lavorativa chiuderli in un cassetto con chiave.

10 Politica BYOD (Bring your Own Device)

Il Titolare autorizza l'installazione e l'uso di dispositivi personali come computer, smartphone e/o tablet ai propri dipendenti per accedere esclusivamente alle risorse di posta elettronica, ai servizi Internet e agli applicativi del Titolare. L'accesso e l'uso continuativo dei servizi di posta è permesso a condizione che ogni utente legga, sottoscriva, rispetti e segua questa e altre politiche e procedure che riguardano l'uso dei servizi forniti.

10.1 Condizioni generali per l'accesso BYOD ai servizi del Titolare

Fatta eccezione per la posta elettronica, qualsiasi download o trasferimento di dati a dispositive personali è proibito o impedito dal sistema di sicurezza.
Gli incaricati non devono eseguire il "*jailbreak*" (iOS) o il "*rooting*" (Android), installando software che permette di eludere le funzioni e i controlli di sicurezza propri dei dispositivi.
Gli incaricati non devono condividere alcun contenuto lavorativo presente sul dispositivo con altri o con i propri familiari.
Gli incaricati devono cancellare qualsiasi file lavorativo che potrebbe inavvertitamente essere scaricato e salvato sul dispositivo.
Non è permesso rimuovere qualsiasi sistema di sicurezza concordato e implementato collegato a questa policy.
Il Titolare adotta sistemi appropriati per verificare che l'uso dei dispositivi personali sia compatibile con le politiche indicate sopra.

11 Restituzione dei beni

Alcuni beni del Titolare sono affidati e controllati dagli incaricati per eseguire le proprie mansioni. Questa politica si applica a tutti gli incaricati che interrompono, anche temporaneamente (es. ferie), l'attività lavorativa e serve ad assicurarsi che i beni del Titolare e temporaneamente assegnati rimangano nelle disponibilità del Titolare.

11.1 Requisiti

Quando il rapporto dell'incaricato con il Titolare si interrompe, anche temporaneamente (es. ferie), tutti i beni devono essere restituiti al Titolare che ne verifica lo stato d'uso al momento della restituzione.

12 Politica di gestione delle password

Le *best practites* per la selezione della password sicura sono essenziali. A tutti gli incaricati viene richiesto di adottare le pratiche seguenti quando si impostano e si gestiscono le proprie password:

1. rendere le password difficoltose da indovinare per chiunque, usando lettere maiuscole, minuscole e numeri;
2. rivelare il proprio user ID solo se richiesto da personale autorizzato come gli amministratori di rete o personale del servizio Reparto IT che sta lavorando a una richiesta di supporto. In tal caso la password deve essere modificata al termine dell'assistenza;
3. mantenere riservate tutte le password;
4. non fornire la propria password a nessuno. Non fornirla al proprio responsabile, a familiari, a terzi in generale o qualsiasi altro individuo. L'uso di password altrui o la comunicazione della propria password può causare un provvedimento disciplinare;
5. cambiare la password ogni volta che c'è il sospetto di compromissione;
6. cambiare la password fornita dal Responsabile IT al primo collegamento;
7. l'utente è responsabile di qualsiasi attività svolta attraverso il proprio User ID e password;
8. non permettere a nessuno di osservare la tastiera quando si inserisce una password;
9. se la password è cambiata o è stata resettata e l'utente non l'ha richiesto, avvertire il responsabile IT dell'accaduto.

13 Politica di pulizia dello schermo e scrivania

Informazioni sensibili o confidenziali, dati personali e altre informazioni, conservate sia elettronicamente, sia in forma cartacea, devono essere conservate in modo sicuro quando il personale è assente dalla propria postazione di lavoro e alla fine di ogni giornata.
Questa politica si applica in particolar modo alle aree di lavoro, come scrivanie o tavoli, su cui non dovrebbero essere lasciate incustodite informazioni confidenziali, sensibili o che contengono informazioni personali.

13.1 Requisiti

Le scrivanie devono essere pulite alla fine di ogni giornata lavorativa da qualsiasi informazione di identificazione personale o riservata. I fascicoli che contengono informazioni riservate devono sempre essere riposti sotto chiave in cassetti della scrivania, armadietti o stanze sicure appositamente progettate.
È necessario assicurarsi che i PC siano posizionati altrove rispetto alle aree pubbliche, in modo che persone non autorizzate possano leggere dagli schermi (attraverso le finestre o mentre stazionano nelle aree pubbliche).
Se sono visibili informazioni confidenziali a persone non autorizzate che stazionano in prossimità degli schermi di computer/laptop, chiedere di allontanarsi per proteggere la confidenzialità di quelle informazioni.
Se bisogna lasciare un messaggio sulla scrivania di qualcun altro, assicurarsi che non contenga informazioni riservate.

14 Denuncia di uso scorretto

In linea con la procedura di gestione degli incidenti, l'uso scorretto deve essere denunciato al responsabile IT. Gli incaricati non devono discutere l'incidente direttamente con l'individuo (o gli individui) coinvolti senza l'autorizzazione del Titolare. Il Titolare, a propria discrezione e secondo le leggi vigenti, può mantiene confidenziali l'identità dell'individuo (o degli individui) che denunciano un uso scorretto.
La procedura per gestire l'uso scorretto (reale o sospetto) potrebbe essere eseguita da un'entità indipendente.

15 Allegato 1

ACCETTAZIONE DELLA "POLICY BYOD"

Io sottoscritto/a (nome e cognome) _____ in qualità di **incaricato del trattamento dei dati personali** in quanto lavoratore autorizzato a consultare, modificare, trasmettere, cancellare ovvero compiere qualsivoglia attività di trattamento a dati personale e che agisce nell'ambito dell'autorità che mi viene concessa, ricevuta, letta e compresa nella sua interessa la politica aziendale sull'uso accettabile degli strumenti informatici aziendali e personali (c.d. BYOD), di seguito "*policy*", con la sottoscrizione della presente

DICHIARO

di accettare integralmente il contenuto, le istruzioni e le disposizioni contenute nella policy indicata e di utilizzare i qui indicati strumenti informatici personali per scopi istituzionali impegnandomi a conformare lo strumento e l'attività conseguente alle indicazioni della policy.

MI IMPEGNO

a segnalare senza indugio eventuali modifiche, dismissioni, perdite accidentali, furti, smarrimenti o aggiunte ai BYOD indicati.

Data: _____ Firma _____

Nome dello strumento BYOD (es. smartphone, tablet, USB):	
Marca:	
Modello:	
Codice IBMEI:	
SIM:	
Sistema operativo:	
Antivirus:	
APP installate per fini istituzionali:	
Uso compatibile per finalità istituzionali (es. e-mail):	

N.B. compilare un numero di dichiarazioni pari al numero di BYOD utilizzati.

Sommario