PROVINCIA DI ORISTANO

DISCIPLINARE PER L'UTILIZZO

DEGLI STRUMENTI INFORMATICI

Approvato con deliberazione n. ____ del _____

V.1.0 del 29 maggio 2023

1. INTRODUZIONE

La Provincia di Oristano, nell'espletamento della propria attività istituzionale, opera prestando la massima attenzione alla sicurezza dei dati, garantendo elevati livelli di sicurezza del proprio sistema informatico, con l'adozione di idonee misure organizzative, tecnologiche e operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informatico.

Il presente documento disciplina l'utilizzo degli strumenti informatici della Provincia da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano strumenti informatici dell'Ente.

2. PRINCIPI GENERALI

Gli strumenti informatici sono assegnati al personale dell'Ente per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e comportamenti adeguati ai compiti assegnati, nel rispetto del Codice di comportamento dei dipendenti della Provincia di Oristano, approvato con delibera G.P. n. 13 del 21.01.2014, delle normative e direttive interne.

Nello svolgimento della propria attività lavorativa, il personale è tenuto al rispetto delle seguenti istruzioni generali:

a) effettuare la propria attività secondo le disposizioni dell'Ente e le istruzioni ricevute;
b) custodire con diligenza la strumentazione informatica assegnata, segnalando tempestivamente alle strutture preposte ogni danneggiamento, smarrimento o furto;
c) mantenere la riservatezza sulle informazioni e sui dati personali trattati durante lo svolgimento della propria attività;
d) in caso di cessazione dal servizio o dalla prestazione svolta per la Provincia di Oristano, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
e) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;

3. REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI

3.1. Credenziali di autenticazione al dominio

L'accesso al sistema informatico della Provincia avviene attraverso autenticazione mediante credenziali di dominio.

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato.

Il sistema di controllo degli accessi presente in Provincia di Oristano implementa le seguenti regole:

- composizione di password complesse, che abbiano una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
- modifica della password al primo utilizzo;
- validità minima e massima della password;
- impossibilità di riuso delle ultime password utilizzate;
- blocco dell'utenza dopo un determinato numero di tentativi falliti di inserimento della password.

I dettagli dei requisiti richiesti sull'utilizzo delle password sono riportati nell'allegato A, punto 1 - "Password".

3.2. Utilizzo di applicazioni aziendali

L'accesso alle applicazioni della Provincia e il loro utilizzo devono avvenire secondo le regole dettate dal presente Disciplinare.

All'atto della cessazione/interruzione del rapporto di lavoro o dell'attività lavorativa svolta a qualsiasi titolo per conto della Provincia, ferma restando la disabilitazione all'uso degli applicativi e delle funzionalità da parte del Responsabile del Servizio Informativi dell'Ente, è fatto obbligo di restituzione delle strumentazioni elettroniche (pc portatili, tablet, cellulari, stampanti, kit di firma elettronica ecc.) già affidate per l'espletazione delle funzioni connesse al rapporto di lavoro, previo appuntamento con il Responsabile del Servizio Sistemi Informativi, che effettuerà le verifiche sulle attrezzature e controfirmerà il modulo di cessione originariamente firmato dal dipendente.

In caso di assegnazione temporanea del personale della Provincia presso altra Pubblica Amministrazione, la titolarità della casella di posta elettronica sul dominio dell'Ente potrà essere mantenuta nel rispetto delle disposizioni che regolano l'uso di tale risorsa ai sensi del presente disciplinare. All'atto dell'assegnazione temporanea e durante il relativo periodo di servizio, il Responsabile del Servizio Informativi dell'Ente provvede alla disabilitazione all'uso degli applicativi e funzionalità, fermo restando l'obbligo del dipendente di restituzione della strumentazione informatica già assegnata per lo svolgimento della prestazione lavorativa.

3.3. Postazione di lavoro

Per postazione si intende un sistema tecnologico costituito da un insieme di apparecchiature e di programmi informatici necessari per lo svolgimento delle attività inerenti al rapporto di lavoro con l'Ente.

Le postazioni di lavoro sono gestite dal Servizio Sistemi Informativi dell'Ente. È vietato qualsiasi utilizzo che deturpi o rovini la postazione di lavoro e tutti gli accessori/periferiche in assegnazione.

La postazione di lavoro è provvista di software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.).

L'assegnatario della postazione di lavoro è profilato come utente senza diritti amministrativi.

La postazione di lavoro è provvista del software base approvato dal Responsabile del Servizio Sistemi Informativi. Ulteriori necessità lavorative potranno essere rappresentate al Responsabile del Servizio Sistemi Informativi, che valuterà l'ammissibilità delle richieste.

L'Utente assegnatario della postazione di lavoro è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

a) al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali. In ogni caso, è fatto divieto di utilizzare strumenti informatici forniti dall'amministrazione per fini diversi da quelli connessi all'attività lavorativa o ad essa riconducibili nel caso in cui l'utilizzo possa compromettere la sicurezza o la reputazione dell'amministrazione
b) la postazione di lavoro non deve essere accessibile a soggetti non autorizzati;
c) il personale non deve apportare modifiche alle configurazioni della postazione di lavoro che non siano state preventivamente richieste e autorizzate dal Responsabile del Servizio Sistemi Informativi dell'Ente;
d) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa sugli spazi di condivisione aziendali;
e) durante l'allontanamento dalla postazione di lavoro, il personale deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password;

3.4. Postazione di lavoro portatile

Per quanto riguarda la postazione portatile, valgono tutte le regole già descritte per le postazioni fisse. Si evidenzia che le stazioni di lavoro portatili, utilizzate al di fuori della sede della Provincia, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutto il personale, pertanto, deve custodire con cura e diligenza la postazione di lavoro portatile assegnata ed è responsabile degli eventuali danni provocati all'apparecchiatura in custodia a meno che non venga provato il caso fortuito.

Le postazioni di lavoro portatili devono essere verificate dal Responsabile del Servizio Sistemi Informativi per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. La verifica avviene mediante indicazioni concordate con il Responsabile del Servizio Sistemi Informativi. In caso di significativo rischio di compromissione o/e sicurezza, il Responsabile del Servizio Sistemi Informativi può richiedere all'utente lo spegnimento della postazione di lavoro portatile fino a tale verifica ovvero bloccare il dispositivo da remoto.

3.5. Altri dispositivi

Con riferimento ad altri dispositivi assegnati ai dipendenti, quali smartphone e/o tablet, valgono le medesime regole comportamentali adottate per le postazioni di lavoro.

3.6. Software a corredo

Non è permessa l'installazione di software aziendale con licenza Provincia di Oristano su dispositivi privati.

3.7. Navigazione in internet

La navigazione in Internet è messa a disposizione del personale come fonte di informazione per le finalità di documentazione, ricerca e studio, utili per lo svolgimento della prestazione lavorativa.

Qualsiasi operazione effettuata sulla rete esterna (accesso a siti web per necessità non inerenti all'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è posta sotto la responsabilità dell'Utente, che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome della Provincia di Oristano.

Ogni Utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare internet per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine della Provincia di Oristano e del personale;
- la navigazione in Internet avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali. In ogni caso è vietato accedere a siti i cui contenuti non siano adeguati all'immagine e al buon nome della Provincia di Oristano.

Al fine di prevenire l'accesso a siti web e risorse internet potenzialmente nocivi, per la navigazione dalla rete aziendale la Provincia adotta soluzioni di sicurezza basate su filtri e decriptazione delle informazioni della navigazione Internet attraverso i quali l'accesso a specifiche e determinate categorie di siti è bloccato a priori. Al fine di prevenire il download di file o pagine web contenenti codici malevoli, la Provincia adotta soluzioni di sicurezza basate su tecnologie antimalware che effettuano la scansione dei contenuti della navigazione Internet e bloccano il download del contenuto in caso di rilevazione di codice malevolo.

3.8. Posta elettronica

Tutti i dipendenti sono dotati di una casella di posta elettronica sul dominio della Provincia di Oristano (nome.cognome@provincia.or.it). Le caselle devono essere utilizzate per l'esercizio della propria attività lavorativa.

L'Ente ha una unica casella di posta elettronica istituzionale certificata e il suo utilizzo in ambito generale o funzionale ad applicazioni è garantito dal Settore Affari Generali.

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni, come indicato nell'allegato A, punto 2 - "Posta elettronica e UC Netiquette".

Il sistema di posta elettronica prevede:

- la possibilità di imporre limiti all'utilizzo del servizio, ad esempio sul numero dei destinatari di un messaggio, sulla dimensione degli allegati che sarà possibile inviare e/o sulla dimensione complessiva della casella di posta elettronica.
- una scansione di sicurezza dei messaggi mediante strumenti automatici, al fine di prevenire la diffusione di e-mail contenenti malware e/o phishing; a fronte di tale controllo si potrebbe rendere necessario l'accesso, da parte dell'amministratore di sistema, ai singoli messaggi identificati come potenzialmente malevoli;
- un sistema automatico di classificazione dei messaggi ricevuti (spam o posta indesiderata), in cui confluiscono tutti i messaggi non reputati leciti dall'algoritmo antispamming.

Nell'utilizzo del servizio il dipendente ha l'obbligo di:

- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- inviare le e-mail esclusivamente a nome proprio. Si ricorda che è considerato mittente il proprietario della casella da cui è inviata l'e-mail, anche in presenza di altri nominativi;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine della Provincia o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione;

- evitare di creare o rispondere ad appelli o richieste non pertinenti all'attività lavorativa;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi o a liste di distribuzione interne alla Provincia;
- evitare l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
- evitare di diffondere, all'esterno della Provincia di Oristano, indirizzi di posta elettronica di terzi, per motivi non legati all'attività lavorativa.

Per assicurare la disponibilità di informazioni in caso di assenza improvvisa o prolungata di un dipendente, fermo restando che i contenuti delle e-mail sono ordinariamente consultabili esclusivamente da parte del titolare della casella, vengono adottate le seguenti misure di tipo tecnologico:

- possibilità di attivazione da parte del dipendente, in caso di sua assenza prolungata, della funzione di risposta automatica con invito al mittente a prendere contatto con l'Ufficio competente della Provincia di Oristano

Ulteriori dettagli sull'utilizzo della posta elettronica sono riportati nell'allegato A, punto 2 - "Posta elettronica e UC Netiquette".

3.9. Servizi di Unified Communication (chat, messaggistica, videoconferenza, telefonia)

Gli strumenti di Unified Communication (Comunicazione Unificata, abbreviata in UC), oltre alla posta elettronica, comprendono la chat, la telefonia, la videoconferenza e la collaborazione sui documenti.

L'oggetto che transita nella UC è la comunicazione.

I dipendenti vengono identificati con il proprio Username, che coincide con l'indirizzo di posta elettronica. Il dipendente che invita ospiti esterni a partecipare alla comunicazione (chat o videoconferenza) oppure condivide con tali ospiti l'indirizzo e-mail o il numero telefonico aziendale, si assume la responsabilità di tale invito o condivisione ed è tenuto a comunicare, in anticipo, agli altri partecipanti la presenza di questi ultimi.

Durante l'utilizzo di tali strumenti è opportuno adottare comportamenti consoni, come indicato nell'allegato A, punto 2 - "Posta elettronica e UC Netiquette".

Il sistema di UC prevede la possibilità di inviare messaggi, effettuare videoconferenze, telefonare e, previo consenso di tutti i partecipanti, registrare ognuna delle suddette comunicazioni. I partecipanti alla comunicazione hanno la responsabilità del proprio comportamento e del rispetto della netiquette, anche qualora supportati tecnicamente dal Responsabile del Servizio Sistemi Informativi dell'Ente. I partecipanti, inoltre, sono responsabili della manutenzione dei documenti e della cancellazione dei dati non più necessari. La chat è persistente, pertanto ne rimane traccia come da termini di utilizzo.

3.10. Servizi Cloud e Spazi di condivisione di rete aziendale

Gli spazi di condivisione file server (on premise) o cloud, **devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo**. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali, a seguito di guasti alle postazioni di lavoro.

In caso di comprovato pericolo per la sicurezza dei sistemi, la Provincia di Oristano potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni presenti negli spazi di condivisione dei dipendenti, dandone successiva e tempestiva comunicazione agli interessati.

3.10.1. SERVIZI CLOUD FORNITI DA AZIENDE TERZE

La Provincia di Oristano fornisce a tutti gli Utenti il servizio di cloud storage specificato nell'allegato A, punto 3 – "Servizi cloud forniti".

3.11. Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.)

L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative. Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica antivirus, per permettere al sistema di completare la verifica di sicurezza che non può essere interrotta dal dipendente. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, per non danneggiare e rendere illeggibili i dati.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto la responsabilità dell'utilizzatore, che è tenuto a rivolgersi al Responsabile del Servizio Sistemi Informativi per le opportune configurazioni di sicurezza e/o crittografia del dispositivo.

È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

Il dipendente è tenuto a informare immediatamente il proprio dirigente, il Responsabile del Servizio Sistemi Informativi e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

I supporti rimovibili (pen drive, schede di memoria, hard disk rimovibili, etc.) devono essere custoditi con la massima diligenza e riservatezza e non devono essere lasciati incustoditi o facilmente accessibili.

Nel momento in cui l'Utente non ha più bisogno del supporto, sia esso riscrivibile o non riscrivibile, è tenuto a restituirlo al Responsabile del Servizio Sistemi Informativi.

3.12. Strumenti di firma digitale

L'uso della firma digitale, anche remota, è strettamente personale e non cedibile a terzi.

3.13. Comportamenti non consentiti

Sono vietati a tutti i dipendenti i seguenti comportamenti:

a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche della Provincia di Oristano e/o lo scambio di comunicazioni mediante falsa identità;
b) l'installazione, sulla postazione di lavoro in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato dal Responsabile del Servizio Sistemi Informativi;
c) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;
d) l'allontanamento dalle postazioni di lavoro senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della postazione di lavoro);
e) la modifica delle configurazioni di base dei dispositivi assegnati dalla Provincia senza l'autorizzazione preventiva del Responsabile del Servizio Sistemi Informativi;
f) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

3.14. Protezione contro furti e danneggiamenti

Tutte le postazioni di lavoro portatili e i dispositivi mobili devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti.

Il dipendente è tenuto a informare immediatamente il dirigente responsabile, Responsabile del Servizio Sistemi Informativi e, qualora vi sia la possibilità di una violazione di dati personali, il Responsabile della Protezione dei Dati di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

3.15. Comportamento in caso di assenza programmata

In caso di assenza programmata, al fine di garantire la continuità del servizio, il dipendente si impegnerà a:

- rendere disponibile, ove necessario, la relativa documentazione su una share condivisa dell'ufficio;
- attivare eventualmente la funzione di risposta automatica, utilizzando un messaggio contenente il periodo di assenza e l'eventuale contatto alternativo.

4. SICUREZZA E PROTEZIONE DATI

Al lavoratore viene assicurato, attraverso le piattaforme informatiche in uso, lo stesso livello di sicurezza dei dati, sia con il lavoro in presenza che con la modalità di lavoro a distanza.

Questo livello di sicurezza è garantito attraverso diverse misure adottate dalle aziende coinvolte, sia dalla piattaforma Microsoft365, che dalle procedure contabili e documentali erogate in cloud e on premise.

Il trasferimento di dati al file server avviene tramite un tunnel VPN SSL/VPN IPSec attivato tramite l'applicativo VPN che si interfaccia con il firewall centrale.

Il lavoratore è responsabile del rispetto della riservatezza sulle informazioni di cui è in possesso per lo svolgimento dell'attività lavorativa. In particolare, egli deve assicurarsi che, in occasione delle operazioni di trattamento effettuate, i dati personali non siano soggetti a rischi di distruzione o perdita anche accidentale e si assicurerà che le informazioni non siano accessibili a persone non autorizzate o che vengano svolte operazioni di trattamento non consentite. Il lavoratore è tenuto al trattamento dei dati personali, alla riservatezza dai dati e delle informazioni aziendali in possesso e/o disponibili nel sistema informativo aziendale, nel rispetto dei compiti assegnati.

1. PASSWORD CRITERI DI SICUREZZA

Le password devono soddisfare i seguenti requisiti e criteri:

a) COMPLESSITÀ

I requisiti di complessità vengono verificati al momento della creazione o della modifica della password:

- non possono contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente.
- devono contenere caratteri appartenenti ad almeno tre delle quattro categorie seguenti:
  - caratteri maiuscoli dell'alfabeto italiano (A-Z);
  - caratteri minuscoli dell'alfabeto italiano (a-z);
  - cifre decimali (0-9);
  - caratteri non alfabetici (ad esempio: !, $, #, %);

b) LUNGHEZZA PASSWORD MINIMA: 8 CARATTERI

c) MODIFICA, VALIDITÀ E BLOCCO DELLA PASSWORD

- necessità di modifica al primo utilizzo;
- validità massima: 90 giorni;
- validità minima: 2 giorni (determina il periodo di tempo in cui deve essere utilizzata una password prima che l'utente possa modificarla);
- impossibilità di riuso delle ultime 4 password utilizzate;

2. POSTA ELETTRONICA E UC NETIQUETTE

- Assicurarsi di aver letto accuratamente e compreso il messaggio a cui si risponde.
- Rispondere solo a chi ci ha scritto, coinvolgendo terzi unicamente se necessario o se funzionale all'efficienza dell'ufficio.
- Assicurarsi dei corretti destinatari della comunicazione, onde evitare di coinvolgere persone non interessate.
- Specificare sempre, nel campo "oggetto", l'argomento del proprio messaggio in modo chiaro, sintetico e inequivocabile.
- Scrivere in modo chiaro e sintetico.
- Inserire allegati solo se non disponibili in spazi di condivisione aziendale o reperibili in rete.
- Chiedere al destinatario la conferma di lettura unicamente se necessario.
- Rileggere e controllare il proprio messaggio prima di inviarlo, per evitare errori materiali che possano dare un'impressione di scarsa accuratezza.
- Smussare asperità o toni che possano risultare irritanti o offensivi.

- Essere certi dell'univocità dei contenuti, per non essere fraintesi. Inoltre, con particolare riferimento ai servizi di UC:
    - adoperare la messaggistica per comunicazioni brevi;
    - controllare frequentemente il proprio stato di presenza e adeguarlo alla propria corrente attività;
    - controllare lo stato di presenza degli utenti con cui si vuole comunicare ed evitare, quando non necessario, di attivare una comunicazione sincrona se l'utente è già impegnato;
    - silenziare il microfono durante gli interventi altrui;
    - utilizzare lo strumento alzata di mano - ove presente – per chiedere la parola, in particolare nelle comunicazioni affollate, onde evitare sovrapposizioni;
    - adoperare gli strumenti adatti per selezionare uno o più utenti a cui rispondere privatamente, qualora non fosse necessario coinvolgere altri all'interno di una discussione di gruppo;
    - qualora si effettui una videochiamata in luoghi in cui sono presenti persone estranee alla conversazione, evitare inquadrature e registrazioni video o audio che ledano la privacy altrui.

3. SERVIZI CLOUD

La Provincia di Oristano fornisce a tutti gli utenti il servizio di cloud storage "Microsoft One Drive", accessibile tramite browser, applicazione desktop e mobile sia dalla rete aziendale che dalla rete internet. L'accesso è effettuato mediante le credenziali di Microsoft365 e l'utilizzo del servizio è consentito esclusivamente per la memorizzazione di file attinenti all'attività lavorativa. L'installazione e l'utilizzo di altri sistemi di cloud storage concorrenti (ad es. Dropbox, Google Drive, etc.) devono essere preventivamente richiesti con opportuna motivazione e autorizzati dal Servizio Sistemi Informativi.

PROVINCIA DI ORISTANO

VERBALE DI CONSEGNA DI ATTREZZATURE INFORMATICHE

Il/La sottoscritto/a _____ , dipendente della Provincia di Oristano

DICHIARA

- di aver ricevuto le attrezzature informatiche così come da scheda cespite allegata al presente verbale;
- di assumere la piena responsabilità e custodire con diligenza la strumentazione informatica assegnata, nel rispetto di quanto regolamentato nel Disciplinare per l'utilizzo degli strumenti informatici della Provincia di Oristano;
- che restituirà i beni integri a semplice richiesta motivata e, comunque, in caso di cessazione dal servizio o dalla prestazione svolta per la Provincia di Oristano.

Data _____

Il Consegnatario

_____