parco nazionale dell'alta murgia

DETERMINAZIONE DIRIGENZIALE (COPIA)

N. **326/2019**	del **03-12-2019**

OGGETTO	**APPROVAZIONE DISCIPLINARE SULL'UTILIZZO DELLE ATTREZZATURE INFORMATICHE, DELLA POSTA ELETTRONICA E DELLA RETE INTERNET SUI LUOGHI DI LAVORO E DISPOSIZIONI DISCIPLINARI SUL LAVORO STRAORDINARIO**

IL DIRETTORE

VISTO che:

-In data 8.10.2019 il Consiglio Direttivo ha preso atto dello stato della contrattazione integrativa oltre che dell'approvazione in sede sindacale del Piano per la Formazione dei dipendenti, la formulazione di tre gruppi di lavoro e il modello organizzativo con ipotesi di regolamento di organizzazione degli Uffici.

-nella stessa seduta si è assunta una bozza di disciplinare in merito all'uso interno delle attrezzature informatiche, della posta e della rete internet a seguito dell'assetto in corso delle reti informatiche e dei programmi in uso agli Uffici;

-a seguito della riunione sindacale del 12.11.2019 sulla contrattazione integrativa decentrata oltre alla approvazione dell' attuazione degli art. 77-78 e 79 del CCNL 2016-18 per cui si è concordato di attuare quanto previsto sulla maggiorazione del premio entro un valore idoneo rispetto alle attività svolte e alle professionalità p/c , applicate al 50% del personale, oltre alle misure di disincentivazione per elevati tassi di assenze anche rispetto al raggiungimento degli obiettivi di miglioramento, facendo salvi i lavoratori che nel 2018 hanno svolto le loro attività presso altre istituzioni ;

-nella stessa riunione in merito allo straordinario dipendenti impegnati in attività di diretta collaborazione con gli Organi istituzionali, la Direzione, chiede di poter, elevare il limite fissato in presenza di esigenze eccezionali e per specifiche categorie di lavoratori a rischio, nonché la ripartizione, sempre da parte della Direzione, delle risorse tra i diversi Servizi in base alle citate attività dei gruppi di lavoro come approvati nella precedente riunione del 10.09.2019;

-di fatto in verbale risulta "tale ripartizione sarà commisurata sulla base del numero dei dipendenti assegnati a ciascun Servizio e delle esigenze di lavoro, tenuto conto degli obiettivi dell'Ente"…

-a maggiore chiarimento sulle modalità di utilizzo delle disposizioni sul lavoro straordinario è stato approvato un apposito disciplinare che allegato alla presente ne forma parte integrante e sostanziale

VISTO il Verbale della riunione sindacale del 12.11.2019 sulla contrattazione integrativa decentrata;

VISTO il CCNL del Comparto Funzioni Centrali – Enti Pubblici non Economici;

VISTO Il D.Lgs. 30 marzo 2001, n. 165 recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle Amministrazioni Pubbliche e ss.mm.ii";

CONSIDERATO che al fine di una maggiore efficacia/efficienza, e nel rispetto delle normative vigenti in materia dell'uso interno delle attrezzature informatiche, della posta e della rete internet è stato predisposto apposito disciplinare come per il lavoro straordinario all'interno dell'Ente;

CONSIDERATO che occorre procedere all'assunzione dei citati provvedimenti;

Tutto ciò premesso, quale espletata istruttoria,

DETERMINA

Le premesse sono parte integrante del presente provvedimento;

DI APPROVARE il "DISCIPLINARE SULL'UTILIZZO DELLE ATTREZZATURE INFORMATICHE, DELLA POSTA ELETTRONICA E DELLA RETE INTERNET SUI LUOGHI DI LAVORO" che allegato al presente provvedimento ne formano parte integrante e sostanziale

DI APPROVARE altresì le DISPOSIZIONI DISCIPLINARI SUL LAVORO STRAORDINARIO stabilite nel verbale della riunione sindacale del 12.11.2019 che allegato alla presente ne forma parte integrante e sostanziale

DI DICHARARE il presente provvedimento immediatamente esecutivo.

DI PUBBLICARE il presente provvedimento sul sito web di questo Ente.

IL DIRETTORE
F.TO DOMENICO NICOLETTI

COPIA CONFORME ALL'ORIGINALE
(sottoscritto con firma digitale ai sensi del D.Lgs. 82/2005 e ss.mm.ii.)

IL DIRETTORE
DOMENICO NICOLETTI

ALLEGATO 1

Fermo quanto stabilito ed approvato dall'incontro sindacale del 12 novembre 2019, del CCNL, del contratto integrativo e nella circolare n.1 del 2019, si approva nella stessa data il seguente disciplinare per le prestazione dello straordinario:

1. La prestazione di lavoro straordinario deve essere preventivamente autorizzata in forma scritta con firma autentica dal Direttore o dal Responsabile dell' Ufficio, sulla base delle effettive esigenze di servizio, rimanendo esclusa ogni forma generalizzata di autorizzazione e nei limiti del monte ore autorizzabile, tenendo conto delle disponibilità delle somme assegnate ad ogni singolo Ufficio.
2. Le prestazioni di lavoro straordinario possono dare luogo, a domanda del dipendente, a riposo compensativo, compatibilmente con le esigenze organizzative e di servizio, da usufruire normalmente entro i quattro mesi successivi; la disciplina del presente comma si applica ai lavoratori che non abbiano aderito alla banca delle ore.
3. Il lavoratore è tenuto a registrare l'ora d'entrata e d'uscita sul dispositivo marca tempo, salvo il caso in cui l'inizio della prestazione che da luogo al lavoro straordinario sia in prosecuzione del completamento dell'orario ordinario, oppure quando le circostanze non lo consentono (ad es. presidio di stand per più giorni per manifestazioni che rendono oggettivamente impossibile il rientro in sede, ovvero partenza o rientro in sede al di fuori dell'orario di servizio).
4. Solo in caso di urgenze e se rientra nello sforamento di max due ore, per fronteggiare particolari emergenze, il dipendente può effettuare il lavoro straordinario senza la preventiva autorizzazione; in tal caso, il giorno seguente lavorativo, è tenuto a motivare l'urgenza al Direttore/Responsabile di Area, il quale rilascia, previa verifica dell'effettiva necessità della prestazione, autorizzazione a sanatoria.
5. Entro il giorno 10 del mese successivo a quello in cui è stato effettuato il lavoro straordinario, ciascun dipendente richiede all'amministrazione la liquidazione delle ore effettuate nel corso del mese precedente (ovvero comunica di voler trasformare le ore di straordinario in riposo compensativo o, qualora vi abbia aderito, di volerle accantonare nella banca delle ore), compilando apposito modulo e presentando le relative autorizzazioni. In ogni caso la mancata compilazione del modulo determinerà l'automatico accantonamento delle ore di straordinario effettuate nella banca delle ore.
6. L'ufficio del Personale liquiderà esclusivamente le richieste conformi alla presente disciplina. La liquidazione avverrà con le competenze del mese successivo a quello in cui lo straordinario è stato effettuato.
7. Il Direttore può in ogni momento in presenza di esigenze eccezionali o per specifiche categorie di lavoratori a norma dell’art. 25, comma 3 integrativo CCNL 2016/2018, elevare il limite fissato per lo straordinario entro le disponibilità dell’Ufficio di appartenenza, con particolare riferimento ai dipendenti impegnati in attività di diretta collaborazione con gli Organi istituzionali e soggetti a rischio, nonché la nuova ripartizione, sempre da parte della Direzione, delle risorse tra i diversi Uffici; tale ripartizione sarà commisurata sulla base del numero dei dipendenti assegnati a ciascun Ufficio e delle esigenze di lavoro, tenuto conto degli obiettivi dell’Ente.

DISCIPLINARE SULL'UTILIZZO DELLE ATTREZZATURE INFORMATICHE, DELLA POSTA ELETTRONICA E DELLA RETE INTERNET SUI LUOGHI DI LAVORO

Il Parco Nazionale dell'Alta Murgia, in persona del Direttore, Prof. Domenico NICOLETTI, in qualità di datore di lavoro

PREMESSO CHE

- Il Parco Nazionale dell'Alta Murgia promuove l'utilizzo della rete informatica e telematica, di internet e della posta elettronica, quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente;

- al Parco Nazionale dell'Alta Murgia, in qualità di datore di lavoro, compete assicurare la funzionalità e il corretto impiego delle attrezzature informatiche, della rete Internet e della posta elettronica sui luoghi di lavoro, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;

- al Parco, quale Titolare del trattamento, compete adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di dati e sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt.15, 31 ss., 167 e 169 D.Lgs.196/03);

-L'uso delle attrezzature informatiche è consentito nel rispetto del Regolamento dei Servizi Informatici dell'ente, delle Norme di "buon uso" dei servizi di rete secondo lo spirito dell'RFC 1855 (Request for Comment 1855 – "Netiquette Guidelines") e secondo le direttive emanate dal Gruppo di Armonizzazione Reti della Ricerca (GARR);

- l'utilizzo nel contesto lavorativo della rete Internet e della posta elettronica sono in rapido incremento in numerose attività lavorative e le tecnologie dell'informazione permettono di svolgere trattamenti di dati personali ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, di cui i lavoratori devono avere conoscenza e consapevolezza;

- l'impiego di Internet da parte dei lavoratori può formare oggetto di analisi e verifiche ed anche i servizi di posta elettronica sono suscettibili di controlli; le informazioni così trattate possono contenere dati personali, in alcuni casi anche sensibili, riguardanti lavoratori o terzi, identificati o identificabili;

- è indispensabile, anche in tale ambito, rispettare il principio di correttezza, di cui all'art.11, lett.a) D.Lgs.196/03, secondo cui le caratteristiche principali del trattamento dei dati personali devono essere rese note ai lavoratori.

Tutto ciò premesso e considerato, il Parco Nazionale dell'Alta Murgia, in persona del Direttore

ADOTTA
il presente disciplinare sull'impiego delle attrezzature informatiche, di Internet e della posta elettronica sui luoghi di lavoro, per conformare i trattamenti di dati personali effettuati dall'Ente alle disposizioni vigenti, al fine di verificare il corretto utilizzo di tali strumenti nel contesto lavorativo.

Art.1
Oggetto e Finalità
Il presente disciplinare rientra tra le misure organizzative, tecniche, procedurali e di sicurezza, adottate dal Parco dell'Alta Murgia, quale Titolare del trattamento, allo scopo di garantire che i trattamenti di dati personali siano svolti nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone.

Esso descrive le regole e modalità di utilizzo delle attrezzature informatiche e telematiche, di internet e della posta elettronica, da parte dei dipendenti e dei collaboratori che l'Ente considera corrette e ammissibili nel contesto lavorativo.

L'Ente Parco, attraverso la descrizione chiara e dettagliata delle regole di seguito indicate, intende informare il proprio personale ed i suoi collaboratori sulle corrette modalità di uso della rete Internet e della posta elettronica sui luoghi di lavoro e sulla possibilità e modalità di eventuali controlli, al fine di prevenire utilizzi impropri di tali strumenti nel rapporto di lavoro, con la conseguenza di ridurre all'indispensabile le verifiche successive sui lavoratori.

Nel rispetto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali, tali regole sono dettate per prevenire usi arbitrari degli strumenti informatici dell'Ente, che possono essere fonte di responsabilità anche penali (artt.15, 31 ss., 167 e 169 del Codice).

Art.2
Pubblicità ed aggiornamento
Il presente disciplinare dovrà essere adeguatamente pubblicizzato tra gli utenti, mediante affissione in bacheca sui luoghi di lavoro, in albi e mediante pubblicazione in cartelle condivise nella rete Intranet del Parco.
Per utenti si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato, i collaboratori coordinati e continuativi, il personale con altre forme di rapporto di lavoro e, nei casi strettamente necessari e preventivamente autorizzati, il personale delle ditte esterne che intrattengono rapporti professionali con il Parco Nazionale dell'Alta Murgia.
Questo disciplinare dovrà anche essere periodicamente aggiornato, in considerazione del progresso tecnico, dell'innovazione tecnologica e dell'introduzione di nuovi strumenti informatici.

Art.3
Principi generali
Gli strumenti informatici e telematici assegnati agli utenti sono strumenti di lavoro e come tali non devono essere usati per fini diversi dalla normale attività lavorativa.

L'Ente adotta ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni informatiche e telematiche di sua proprietà.
Ogni utente è responsabile, civilmente e penalmente, del corretto uso degli strumenti informatici e telematici, dei servizi/programmi a cui ha accesso e dei dati trattati ai fini istituzionali.
Il dipendente è altresì responsabile del corretto uso della posta elettronica, anche per quanto attiene la riservatezza dei dati contenuti nelle comunicazioni inviate e ricevute, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e/o della normativa per la tutela dei dati personali.

Art. 4
Definizioni
Ai fini del presente Regolamento si intendono:
per Rete del parco: l'insieme di tutte le reti locali delle strutture dell'ente dirette alla condivisione delle risorse informatiche comuni per l'interscambio di informazioni e per ogni altra applicazione telematica all'interno e all'esterno dell'ente;
per Strumenti informatici: personal computer fissi o mobili, stampanti locali o di rete, prodotti software, dispositivi mobili o altri dispositivi di telecomunicazione e le relative periferiche nonché tutta l'infrastruttura logica e fisica che permette l'interconnessione delle postazioni di lavoro e/o di studio, al fine di agevolare la trasmissione dei dati, compresi tutti gli spazi di rete personali o condivisi messi a disposizione dei dipendenti per svolgere le proprie attività;
per Dispositivo di memorizzazione rimovibile: qualunque dispositivo di memorizzazione che utilizzi supporti rimovibili;
per Aree di memorizzazione personali e/o condivise in rete: spazi messi a disposizione dei dipendenti in relazione all'attività che devono svolgere in base alle loro mansioni;
per Amministratore di sistema: ogni soggetto incaricato dall'ente di gestire un sistema informatico;
per Utente: chiunque utilizzi un Sistema in Rete del parco.

Art.5
Utilizzo delle postazioni hardware-software
Gli utenti sono responsabili del corretto utilizzo e della corretta custodia della postazioni hardware loro assegnate, tenendo presente che ogni utilizzo dei PC non inerente all'attività lavorativa può contribuire ad innescare disservizi, minacce alla sicurezza e inutili costi di manutenzione.
L'accesso agli strumenti informatici è protetto da una password o da altro dispositivo di autenticazione. La password o il dispositivo di autenticazione è strettamente personale e non deve essere ceduto a terzi.
Nell'uso di dispositivi di memorizzazione removibili, l'utente è tenuto ad adottare ogni comportamento utile ad evitare la propagazione di virus.
Sui file server che ospitano le aree di memorizzazione messe a disposizione dei dipendenti vengono svolte regolari attività di back-up e di controllo da parte dell'Amministratore di Sistema appositamente incaricato al fine di garantirne il corretto funzionamento e l'integrità dei dati in esse contenuti. In qualunque momento l'Amministratore di Sistema può, previa segnalazione al Responsabile dell'area di memorizzazione interessata, procedere alla rimozione di ogni file o applicazione ritenuti pericolosi e che impediscono una corretta gestione e manutenzione delle unità di rete.

Analoga procedura si applica anche in caso di assenza prolungata o impedimento dei Responsabili o degli utenti dell'unità di Rete.

In caso di assegnazione di computer portatili, questi devono essere custoditi dagli utenti con la massima diligenza e, quando vengono portati all'esterno dei locali dell'Ente Parco, questi devono essere conservati in un luogo protetto.

Nel caso in cui gli utenti dovessero riscontrare furti, mancanze o anomalie nelle dotazioni informatiche e telematiche assegnate, devono darne immediata comunicazione al proprio responsabile, per l'effettuazione della denuncia alle Autorità competenti.

Al momento della consegna di ogni stazione di lavoro (sia di tipo desktop che portatile) vengono effettuate, da parte del fornitore o dall'Amministratore di sistema, le seguenti operazioni:
● installazione del sistema operativo;
● configurazione dell'accesso alla rete aziendale;
● installazione e configurazione delle periferiche (es. stampante);
● installazione del software antivirus;
● installazione del software di office automation;
● installazione di software aggiuntivo per attività lavorative specifiche dell'utente (es.: programmi di protocollo o disegno tecnico);
● installazione dei software che consentono l'utilizzo delle periferiche presenti sulla rete;
● assegnazione delle credenziali di accesso (user-id e password) con cui l'utente potrà accedere ad internet ed alle risorse delle rete intranet;
Durante l'utilizzo degli strumenti informatici e telematici non è consentito:
● adottare comportamenti che possano determinare danni economici e di immagine all'Ente Parco;
● utilizzare password di accensione (BIOS) per prevenire l'utilizzo del computer;
● accedere ad un personal computer con credenziali di amministratore o diverse da quelle fornite; le credenziali sono peraltro strettamente personali e non devono essere divulgate;
● installare e/o duplicare qualunque software, anche se libero, non fornito o autorizzato dall'Amministratore di sistema, previo assenso della Direzione;
● installare o eseguire programmi che possano determinare il danneggiamento o un sovraccarico dei sistemi e/o della rete;
● alterare le funzionalità (es. indirizzi e protocolli di rete) del collegamento in rete della stazione di lavoro impostata dall'Amministratore di sistema;
● apportare modifiche hardware al personal computer in dotazione;
● memorizzare documenti informatici contrari alle vigenti norme di legge;
● inibire o sospendere, anche temporaneamente, il funzionamento del software antivirus installato sulla stazione di lavoro;
● configurare autonomamente i servizi essenziali già resi in modo centralizzato (es.: DNS, WINS, DHCP, NTP, FTP, HTTP/HTTPS, posta elettronica, accesso remoto, proxy server, etc.);
●tenere comportamenti che possano influenzare negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e/o le prestazioni per gli altri utenti;

● non è consentito al dipendente modificare le caratteristiche hardware e software impostate sul proprio Personal Computer (PC), installare software diverso da quello autorizzato o riprodurre e/o duplicare i programmi informatici.
● ogni altro utilizzo non inerente l'attività lavorativa.
Durante l'utilizzo degli strumenti informatici e telematici è peraltro obbligatorio:
● effettuare una "pulizia" periodica, almeno ogni sei mesi, dei dati contenuti nella memoria del proprio PC, cancellando files inutili o obsoleti;
● spegnere correttamente il personal computer al termine della giornata lavorativa o in caso di assenze prolungate, dato che lasciare inutilmente acceso un calcolatore, oltre a costituire un potenziale rischio di incendio qualora venga lasciato incustodito, rappresenta anche un inutile spreco di risorse energetiche con conseguente aggravio di costi ed inutile danno all'ambiente;
● Ogni qualvolta l'utente si allontani dalla postazione di lavoro è tenuto a rendere il terminale inaccessibile a terzi. I personal computer portatili e i dispositivi mobili assegnati agli utenti devono essere custoditi e protetti come le postazioni di lavoro fisse, avendo altresì cura di mantenere l'integrità dei software installati e dei dati memorizzati.
● utilizzare password che soddisfino i requisiti di complessità (almeno 8 caratteri che prevedano maiuscole, minuscole e numeri), evitando contenuti facilmente individuabili e modificando periodicamente ciascuna password, almeno ogni sei mesi (in caso di trattamento di dati sensibili la password deve essere modificata almeno ogni tre mesi);
● utilizzare screen-saver per la riservatezza dei dati visualizzati e meccanismi automatici di blocco della postazione in caso di inattività per un periodo di 5 minuti;

Art.6
Informativa ex art.13 Codice privacy
Il Parco Nazionale dell'Alta Murgia, in persona del legale rapp.te p.t., quale Titolare del trattamento, tratta i dati personali relativi alla navigazione in Internet ed alla posta elettronica per finalità connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro e per l'eventuale esercizio di diritti in sede giudiziaria.
TIPOLOGIA DI DATI
L'utilizzo di Internet da parte dei lavoratori può formare oggetto di analisi, verifica e ricostruzione, mediante elaborazione di *log file* della navigazione *web* ottenuti da strumenti specifici di registrazione delle informazioni. I servizi di posta elettronica sono ugualmente suscettibili di controlli.
Le informazioni così trattate possono contenere dati personali, anche sensibili, riguardanti lavoratori o terzi, identificati o identificabili.
MODALITÀ DEL TRATTAMENTO
La registrazione e l'elaborazione dei dati avvengono in forma elettronica e cartacea; il trattamento si attua con logiche strettamente correlate alle finalità sopraindicate e comunque in modo da garantire la sicurezza e la riservatezza dei dati. I dati relativi ai *file log* della navigazione web sono temporaneamente memorizzati.
Tali informazioni sono conservate giornalmente nelle copie di *back up*, per le finalità di gestione, manutenzione e sicurezza della rete dell'Ente Parco e annualmente cancellate.
A tali dati possono legittimamente accedere solo gli amministratori di sistema, a seguito di apposita prescrizione del datore di lavoro, salvo il caso di indagini giudiziarie o di polizia.

CONTROLLI

L'Ente Parco, in conformità della legge, si riserva di effettuare controlli occasionali, a campione, per verificare la funzionalità e sicurezza del proprio sistema informativo.
Ove siano riscontrati reiterati abusi nell'uso della rete Internet e della posta elettronica sui luoghi di lavoro, il Parco Nazionale dell'Alta Murgia provvederà ad inoltrare preventivi avvisi collettivi ai dipendenti e solo successivamente, persistendo l'uso improprio, provvederà ad effettuare controlli su singoli dispositivi e postazioni, mediante il personale appositamente individuato ed incaricato.

SICUREZZA DEI DATI E DEI SISTEMI
I dipendenti e collaboratori del Parco, nello svolgimento della loro attività lavorativa, sono tenuti ad utilizzare gli strumenti informatici e le reti telematiche dell'ente nel rispetto delle regole tecniche, procedurali ed organizzative e delle istruzioni impartite dal datore di lavoro, nonché delle misure di sicurezza descritte nel Documento Programmatico sulla Sicurezza (DPS), annualmente adottato dall'ente.
I dipendenti, incaricati del trattamento dei dati, sono tenuti ad adottare tutte le necessarie cautele per assicurare la segretezza della componente riservata della credenziale di autenticazione e la diligente custodia dei dispositivi in loro possesso ed uso esclusivo, allo scopo di evitarne la conoscibilità a soggetti non autorizzati .
I dipendenti e collaboratori non devono lasciare incustodito e accessibile lo strumento elettronico in uso e/ o assegnazione, durante una sessione di trattamento, ciò al fine di evitare l'utilizzo della rete Intranet ed Internet da parte di soggetti diversi non abilitati o autorizzati.

ESERCIZIO DEI DIRITTI
Gli interessati potranno rivolgersi, in ogni momento, al Parco Nazionale dell'Alta Murgia, in persona del legale rappresentante p.t., con sede in via Firenza 10 Gravina in Puglia (BA) in qualità di Titolare del trattamento, per esercitare i diritti previsti dall'art.7 del D.Lgs.196/03.

Art.7
Individuazione di preventive misure organizzative e tecnologiche

Il Parco Nazionale dell'Alta Murgia, quale datore di lavoro e Titolare del trattamento, intende garantire, anche sul luogo di lavoro, la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati, in una cornice di reciproci diritti e doveri ed assicurare l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali. Pertanto, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, il Parco ha predisposto modalità d'uso che, tenendo conto del crescente lavoro in rete, consentono un utilizzo consono di tali strumenti.
In applicazione del principio di necessità, sancito dall'art.3 D.Lgs.196/03, l'Ente Parco ha preferito promuovere opportune misure, organizzative e tecnologiche, per prevenire il rischio di usi impropri della rete Internet e della posta elettronica sul luogo di lavoro, privilegiando tali misure rispetto a strumenti repressivi.
Pertanto, il Parco ha:
- individuato preventivamente a quali soggetti è accordato l'utilizzo della posta elettronica e di Internet;
- determinato quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di loro impiego abusivo;

Art. 8
Misure per ridurre a casi eccezionali i controlli sui lavoratori
Il Parco Nazionale dell'Alta Murgia, quale datore di lavoro, per prevenire la possibilità di analisi, prevista solo in casi limitati, del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'Ente, indica di seguito le necessarie misure per prevenire utilizzi impropri della rete Internet e della posta elettronica sui luoghi di lavoro, al fine di ridurre ad ipotesi eccezionali possibili controlli successivi sui lavoratori.

Art. 9
Regole per il corretto utilizzo della rete Internet e della posta elettronica
In osservanza a quanto stabilito dallo Statuto dei lavoratori sul divieto di controllo a distanza dell'attività lavorativa (art.4 L.300/1970), il Parco non effettua il monitoraggio sistematico delle pagine *web* visualizzate dai lavoratori, né la lettura e la registrazione sistematica delle *e-mail* d'ufficio assegnate ai lavoratori.
Ciò nonostante, al fine di evitare comportamenti non conformi alla corretta esecuzione dell'attività lavorativa ed eventuali abusi nell'utilizzo di Internet e della posta elettronica, l'Ente Parco richiama tutti i dipendenti e collaboratori dell'ente al rispetto delle seguenti vincolanti misure.

Art.10
Misure adottate per la navigazione in Internet
La connessione ad Internet avviene mediante l'infrastruttura di rete aziendale. È vietata qualsiasi altra modalità di connessione ad Internet se non tramite le apparecchiature fornite e con le modalità consentite.
Per la navigazione in Internet da parte dei dipendenti sul luogo di lavoro, Il Parco nazionale dell'Alta Murgia dovrà provvedere:

- ad individuare, anche su indicazione dei dipendenti, le categorie di siti web considerati correlati con la prestazione lavorativa;
- a configurare sistemi e filtri che prevengono determinate operazioni, ritenute estranee all'attività lavorativa e, quindi, non tollerabili, quali l'accesso a determinati siti (inseriti in una *black list)*, e/o il *download* di file musicali o multimediali, o di software aventi particolari caratteristiche (dimensionali, di tipologia di dato, di *licensing*);
- a trattare i dati relativi alla navigazione web dei dipendenti in forma aggregata ed anonima, tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni;
- alla conservazione dei dati per il tempo indispensabile al perseguimento di finalità organizzative, produttive e di sicurezza del sistema informativo dell'Ente;
- a graduare i controlli, escludendo verifiche prolungate, indiscriminate e costanti.

I controlli sull'uso degli strumenti elettronici saranno effettuati evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata, nel rispetto dei principi di pertinenza e non eccedenza.
Nel caso in cui un evento dannoso o pericoloso non sia stato impedito con i preventivi accorgimenti tecnici, il Parco può adottare eventuali misure che consentano la verifica di comportamenti anomali, preferendo comunque un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo si concluderà con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti dell'Ente e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite, oppure con un avviso circoscritto ai dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
In presenza di successive ripetute anomalie saranno effettuati controlli su base individuale.

Art.11
Misure adottate per l'uso della posta elettronica
In merito all'utilizzo della posta elettronica sui luoghi di lavoro, il Parco richiama l'attenzione dei propri dipendenti sulla natura non privata della corrispondenza in ingresso ed in uscita dall'indirizzo di posta elettronica personale (*nome.cognome@parcoaltamurgia.it)* e dagli indirizzi condivisi (ad es. *info@ parcoaltamurgia.it)* e sull'opportunità del loro utilizzo per le finalità connesse all'espletamento dell'attività lavorativa.

Il Parco, al fine di evitare usi impropri e possibili controlli e di dissipare ogni dubbio sull'impiego della posta elettronica nel contesto lavorativo e di connotare l'uso "istituzionale" che il lavoratore, come mittente o destinatario, fa della posta elettronica, operando quale espressione dell'organizzazione datoriale, si riserva la facoltà di realizzare controlli aventi carattere di gradualità, escludendo verifiche prolungate, costanti o indiscriminate.

Art. 12
Utilizzo dei dispositivi mobili
Le richieste di dotazioni per dispositivi mobili devono essere inoltrate alla direzione. Nel caso di tablet e di attivazione servizio dati su smartphone l'autorizzazione deve essere riconfermata dal Direttore.
I dispositivi mobili devono essere utilizzati esclusivamente con la SIM aziendale abbinata. Non è consentito l'uso del dispositivo aziendale con SIM private o di terzi. È inoltre vietato l'utilizzo della SIM aziendale su dispositivi diversi da quelli consegnati dai sistemi informativi.
Art. 13
Regole comportamentali atte a prevenire crimini informatici
Di seguito vengono descritte le principali regole da osservare per evitare di incorrere in comportamenti illeciti o da cui possano derivare rischi per l'ente. Tali regole disciplinano i comportamenti da seguire relativamente ai seguenti aspetti:

- Attività di spam
- Diffusione di virus e malware
- Attacchi informatici e accessi abusivi ai sistemi
- Pubblicazione e diffusione di materiale offensivo, molesto o sovversivo
- Violazione del diritto d'autore e del copyright
- Diffusione di materiale pedo-pornografico
- Frodi informatiche e furto d'identità
- Violazione del segreto aziendale
- Trattamento illecito di dati personali e di traffico

13.2 Attività di spam

Con il termine spam si indica l'invio di messaggi di posta elettronica a un gran numero di destinatari che non ne abbiano specificatamente fatto richiesta o che non abbiano esplicitamente acconsentito a riceverli.
Obiettivo principale dello spamming è la pubblicità: dalle semplici offerte commerciali, a proposte di vendita di materiale pornografico/pedopornografico, fino a tentativi di truffa veri e propri.

13.2.1 Modalità operative spam

Non iniziare o partecipare ad una catena di corrispondenza ("catene di S. Antonio") né aderire a messaggi di tipo "hoax" (burle ricevute via e-mail che fanno leva sulla credulità del ricevente relativamente a storie drammatiche o alla diffusione di presunti virus);
Evitare di diffondere il proprio indirizzo e-mail aziendale attraverso siti, forum, chat, newsletter o quanto altro non pertinente all'attività lavorativa;
Non accettare mai l'invito a rimuovere il proprio nominativo da una mail list per evitare di confermare allo spammer la validità dell'indirizzo mail;
Non aprire i messaggi che appaiono palesemente come spam e cancellarli tempestivamente dalla mailbox;
Eliminare tempestivamente gli allegati a messaggi di posta elettronica se il mittente è sconosciuto o in caso di mittente noto il testo della mail è in una lingua differente da quella attesa o è composto da frasi senza senso;
Segnalare allo specifico servizio interno Ie mail di spam ricevute, secondo le modalità reperibili sull'intranet.
Non disabilitare o inibire il corretto funzionamento del software anti-virus;

13.3 Diffusione di virus e malware

Con virus e malware si intendono programmi malevoli che possono provocare malfunzionamenti e danni ai sistemi informatici dell'ente mettendo a rischio l'integrità, la disponibilità e la riservatezza di dati ed applicazioni ivi residenti.
Nello specifico un virus appartiene alla categoria dei malware ed è un programma che si inserisce all'interno di file eseguibili o in aree particolari del sistema, con la capacità di "riprodursi" e di duplicarsi, senza che l'utente ne sia a conoscenza sfruttandone la sua attività. I virus possono essere più o meno dannosi per il sistema operativo che li ospita, ma, in ogni caso, comportano sempre uno spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.

13.3.1 Modalità operative virus e malware

Non installare né utilizzare software che non sia stato regolarmente acquisito e distribuito tramite i canali aziendali o comunque non autorizzato dai sistemi informativi;
In presenza di documenti di provenienza incerta, contenenti macro, forzare la disattivazione delle stesse;
Eliminare tempestivamente le e-mail di provenienza sconosciuta e/o con contenuto sospetto;
Non eseguire programmi ricevuti come allegati a messaggi di posta elettronica senza preventivamente averli scaricati sulla postazione di lavoro ed averli sottoposti a controllo con antivirus;
Non visitare siti di dubbia reputazione né eseguire il download di file eseguibili se non si conosce la fonte di provenienza e se non si è espressamente autorizzati;
Durante la navigazione Web e/o la lettura delle e-mail, diffidare delle URL particolarmente lunghe contenenti sequenze di valori esadecimale e dialog box che propongono l'installazione di plug-in o applicativi vari, anche se firmati in modo digitale, di cui l'autore è ignoto;

Segnalare prontamente la presenza di eventuali virus secondo le modalità reperibili sulla intranet.

13.4 Attacchi informatici ed accessi abusivi ai sistemi

Per attacchi informatici si intendono eventi che sfruttano le vulnerabilità di un sistema al fine di utilizzare/alterare le informazioni senza averne i privilegi adeguati e/o di compromettere, anche attraverso una ripetizione di sequenze di operazioni lecite, il regolare funzionamento dei sistemi. Sono altresì considerati attacchi informatici quelle azioni volte ad ottenere l'accesso ad un sistema o a uno specifico oggetto al fine di effettuare su di esso operazioni senza essere in possesso dei privilegi necessari, oppure per scopi diversi da quelli per cui l'accesso è stato autorizzato. L'accesso abusivo infatti consiste nell'introdursi in un sistema informatico o telematico protetto da misure di sicurezza ovvero nel mantenervisi contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

13.4.1 Modalità operative attacchi informatici

Adottare la massima accortezza durante l'utilizzo e la conservazione delle credenziali di autenticazione (nome utente, password, smart card ...) di accesso ai sistemi informatici in modo da evitare una possibile perdita di riservatezza;

Provvedere tempestivamente al cambio della password e comunicare al proprio responsabile gerarchico o referente aziendale, anche solo nel caso in cui si abbia un sospetto, la perdita di riservatezza delle credenziali di accesso ai sistemi informatici;

Scegliere una password robusta e difficilmente intuibile da altri, costruendo la stessa sulla base di quanto disposto dalle normative interne;

Non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;

Non lasciare incustoditi documenti contenenti dati riservati e/o informazioni che possono consentire a soggetti terzi di accedere ai sistemi informatici aziendali; in caso di dismissione dei suddetti documenti provvedere tempestivamente alla distruzione degli stessi mediante apposite apparecchiature (es. trita documenti nel caso di documenti in formato cartaceo);

Non accedere né tentare l'accesso ad informazioni per i quali non si possiedono i privilegi autorizzativi;

Mantenere la corretta configurazione della propria postazione di lavoro non alterando le componenti hardware e software predisposte allo scopo, né installando ulteriori software non autorizzati;

Non installare sul proprio personal computer mezzi di comunicazione o altre periferiche proprie senza preventiva autorizzazione (es. modem, masterizzatori, penne usb, hard disk esterni);

Non servirsi di strumenti che consentano di restare anonimi sulla rete (es. TOR);

Non connettere la propria postazione di lavoro ad una rete esterna (wireless, modem) mentre si è contemporaneamente connessi alla rete interna;

Non utilizzare e/o installare software atti a danneggiare o sovraccaricare i sistemi o la rete;

Non utilizzare e/o installare software atti ad intercettare, falsificare, alterare il contenuto di documenti informatici (es. programmi di password recovery, cracking, sniffing, spoofing, serial codes);

Verificare che sui sistemi di propria competenza vengano regolarmente e tempestivamente applicate le patch software di sicurezza distribuite dai vendors e dai Sistemi Informativi tramite "Windows update";

Applicare le regole previste per contrastare la diffusione di virus e mallware.

13.5 Pubblicazione e divulgazione di materiale offensivo, molesto o sovversivo

Si tratta di fenomeni offensivi e lesivi della dignità umana della libertà individuale e della pubblica morale che spaziano dalle molestie (sessuale, morale, minacce in senso generico o a carattere persecutorio) alla discriminazione razziale ed etnica, religiosa, politica e sessuale. Sono, altresì inclusi quei fenomeni che perseguono scopi contrari all'ordine pubblico, che offendono la religione di stato e/o gli ordinamenti statali.

13.5.1 Modalità operative divulgazione materiale offensivo

Non utilizzare i servizi di rete aziendale quali posta elettronica, internet, intranet per inviare, pubblicare e/o memorizzare materiale dal contenuto:

offensivo, quali commenti circa l'orientamento religioso, politico, le origini razziali, il colore della pelle ed in generale che possa essere lesivo della dignità della persona;a sfondo sessuale, pornografico o di natura oltraggiosa;

offensivo nei confronti degli organi istituzionali dello stato;sovversivo contro l'ordine pubblico;

diffamatorio, calunnioso denigratorio e molesto nei confronti di terzi.

13.6 Violazione del diritto d'autore e del copyright

Con il termine "diritto d'autore" si intende l'insieme dei diritti attribuiti all'autore di un'opera dell'ingegno (musica, libri, film) che riconoscono allo stesso, la facoltà esclusiva di sfruttamento economico e/o la diffusione dell'opera medesima.

Ogni opera dell'ingegno presente su Internet appartiene al proprio autore e non è possibile copiarla modificarla o beneficiarne in alcun modo senza il consenso esplicito dello stesso autore, che ne autorizzi, magari regolamentandolo, l'utilizzo.

La tutela sul diritto d'autore si estende anche alle opere informatizzate, in particolare ai programmi per elaboratore e alle banche dati intese come "raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti e individualmente accessibili grazie a mezzi elettronici o in altro modo".

13.6.1 Modalità operative violazione del diritto di autore

Non installare e utilizzare software privi di regolare licenza;

Non scaricare, indebitamente, e/o diffondere video, file musicali e software, giochi o altro materiale protetto da diritto d'autore;

Non è consentito lo scambio mediante la rete aziendale, di materiale audiovisivo, fotografico, cinematografico, informatico protetto da copyright anche se non effettuato a scopo di lucro;

Non è consentito duplicare, distribuire, adattare e trasformare software regolarmente licenziati dall'Ente per usi privati e comunque diversi dall'utilizzo consentito per l'attività lavorativa;

Non utilizzare la posta elettronica o le cartelle condivise di rete, per memorizzare o spedire materiale che violi il copyright;

Non utilizzare un'informazione, un testo, un'immagine all'interno dei propri lavori senza citare esplicitamente la fonte;

Non è consentita la riproduzione, pubblicazione, distribuzione, totale o parziale, di materiale protetto da diritto d'autore;

Non è consentito rimuovere né utilizzare strumenti atti ad eludere le misure tecnologiche di protezione del materiale protetto dal diritto d'autore.

13.7 Diffusione di materiale pedo-pornografico

Le tipologie di reato connesse alla pedo-pornografia on-line riguardano la produzione, divulgazione o diffusione, la commercializzazione, la detenzione e lo scambio di materiale pedo-pornografico intendendo con tale accezione "qualsiasi rappresentazione, con qualsiasi mezzo, di un bambino dedito ad attività sessuali esplicite, concrete o

simulate o qualsiasi rappresentazione degli organi sessuali di un bambino a fini soprattutto sessuali" (Convenzione Internazionale sui Diritti dell'Infanzia).
Rientra nella nozione di pornografia infantile anche il concetto di pedo-pornografia virtuale (immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali).

13.7.1 Modalità operative violazione diffusione materiale pedo-pornografico

Non detenere sulle postazioni aziendali e su altri strumenti di archiviazione di massa (ad es. USB, hard disk, CD-DVD) materiale pedo-pornografico anche virtuale;
Qualora accidentalmente si venisse a conoscenza di materiale illecito di carattere pedopornografico, anche virtuale, è divieto assoluto diffondere i contenuti tramite servizi di rete aziendale (internet, intranet e posta elettronica);
Non scambiare, cedere e/o vendere materiale pedo-pornografico anche virtuale utilizzando i servizi di rete dell'ente;
Segnalare tempestivamente la presenza di materiale pedopornografico al competente organo dell'ente;
Effettuare la segnalazione seguendo le modalità indicate nella normativa aziendale di riferimento e sul portale.

13.8 Frodi Informatiche e furto d'identità

La frode informatica viene perpetrata mediante l'accesso, l'alterazione, la cancellazione a soppressione di dati a programmi informatici effettuati al fine di cagionare un danno (economico a materiale) a terzi e un ingiusto profitto (inteso quale vantaggio relativo ad interessi morali psicologici a patrimoniali) per se stessi a per altri. Questa si distingue dalla truffa in quanto l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), bensì il sistema informatico.
II furto dell'identità è un particolare tipo di frode informatica che permette al truffatore di ottenere una serie di vantaggi (economici a materiali) attraverso l'utilizzo improprio dell'identità altrui, avvalendosi di informazioni sensibili carpite alla presunta vittima (n. carta credito, indirizzo, n. di conto corrente, n. telefonico, ecc.)

13.7.1 Modalità operative frodi informatiche

Non rispondere a messaggi di posta elettronica che richiedono la verifica delle proprie credenziali per l'accesso ai servizi finanziari (di banche a altri istituti finanziari);
Non inserire i propri dati di login cliccando direttamente sui link proposti all'interno di una e-mail, ma digitar l'indirizzo del sito manualmente per essere certi, di non incorrere in siti contraffatti (es. phishing, pharming);
Non cancellare la sottoscrizione ad una mail list di cui non si è certi dell'iscrizione; potrebbe trattarsi di un raggiro da parte di uno spammer per ottenere conferme sulla validità dell'indirizzo e-mail dell'utente;
Utilizzare solo ed esclusivamente le credenziali di accesso assegnate per l'accesso ai sistemi per cui si è autorizzati;
Non scrivere la password su fogli, biglietti od oggetti che vengono lasciati in prossimità del PC (ad es. sul video, sopra 9 sotto la tastiera);
Non cedere a terzi credenziali di autenticazione personali (ad es. nome utente, password, smarlcard) di accesso ai sistemi informatici;
Non comunicare la password per telefono a altro mezzo a soggetti che si presentano come colleghi, tecnici a supervisari;
Non aprire mai allegati presenti su e-mail ritenute sospette in quanto è possibile che tali allegati una volta aperti, installino un programma che permettere a soggetti terzi di

accedere alle informazioni riservate presenti sulla postazione di lavoro nonchè di visualizzare tutto ciò che viene digitato sulla tastiera del computer (es. keylogging);
Utilizzare e verificare l'aggiornamento dei programmi (antivirus, browser) installati sulla propria postazione di lavoro;
Verificare prima di accedere sul sito web desiderato che sia stata avviata una sessione protetta (es. accertandosi che l'indirizzo web cominci con https);
Non intervenire in modo fraudolento su dati, informazioni a programmi contenuti in un sistema informatico/telematica;
Proteggere i documenti informatici contro tentativi di falsificazione mediante strumenti di firma digitale e crittografia quando previsto;
Non fornire i propri dati personali a società di dubbia reputazione a comunque accettarsi sempre della veridicità del sito web prima di inserire i propri dati sensibili (es. numero carta di credito);
Classificare e gestire correttamente le informazioni aziendali, sotto il profilo della riservatezza, secondo quanto previsto da apposita normativa interna;
Segnalare tempestivamente alla competente struttura aziendale tutti i casi di truffa informatica di cui si viene a conoscenza durante l'espletamento delle proprie mansioni.

Art. 14

Controlli da parte del datore di lavoro

Qualora le preventive misure suindicate non fossero sufficienti ad evitare comportamenti scorretti o anomali, il Parco Nazionale dell'Alta Murgia, in qualità di datore di lavoro si riserva di effettuare, attraverso soggetti appositamente individuati, gli eventuali necessari controlli.
I controlli saranno effettuati nel rispetto del principio di pertinenza e non eccedenza (art.11, I co. lett.d) D.Lgs.196/03), con esclusione di controlli prolungati, costanti o indiscriminati.
Tali verifiche, finalizzate esclusivamente a contrastare usi impropri della rete Internet e della posta elettronica e/o eventuali comportamenti illeciti, fonte di responsabilità, verranno effettuati con gradualità.
In primo luogo, saranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole; solo successivamente, ripetendosi l'anomalia, l'Ente potrebbe passare a controlli su base individuale, previa contestazione scritta indirizzata al dipendente.
Si rinvia alla normativa vigente per ciò che concerne le sanzioni disciplinari applicabili in merito alle eventuali violazioni accertate.

Art.15

Conservazione dei dati di navigazione

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici sarà effettuata solo per finalità specifiche e comprovate e per il periodo di tempo indispensabile al perseguimento di tali finalità.
L'eventuale prolungamento dei tempi di conservazione avrà carattere eccezionale e potrà avvenire esclusivamente in relazione:
- ad esigenze tecniche o di sicurezza del tutto particolari;

- all'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire le predette finalità ed avverrà con logiche strettamente correlate agli obblighi, compiti e finalità esplicitati.

Art.16

Individuazione dei soggetti preposti

Il Parco Nazionale dell'Alta Murgia provvederà a designare espressamente i soggetti autorizzati ad effettuare i tipi di controlli ammessi e le relative modalità di esecuzione, impartendo loro precise istruzioni.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati, in particolare, gli incaricati della manutenzione, di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

I soggetti che operano quali Amministratori di sistema e gli incaricati della manutenzione, cui siano affidate le operazioni connesse al regolare funzionamento dei sistemi, sono dotati di capacità ed esperienza in merito ai profili tecnico-gestionali e di sicurezza delle reti, ai principi di protezione dei dati personali ed al segreto nelle comunicazioni