v. EN

Mobile Device Acceptable Use Policy

Purpose

This policy defines standards, procedures, and restrictions for any and all end users with legitimate business uses connecting mobile devices to THE NEW PAGAN DAWN's corporate network, digital resources, and data. The mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- *Smartphones*
- *Other mobile/cellular phones*
- *Tablets*
- *E-readers*
- *Portable media devices*
- *Portable gaming devices*
- *Laptop/notebook/ultrabook computers*
- *Wearable computing devices*
- *Any other mobile device capable of storing corporate data and connecting to a network*

In order to enforce security and remote device management, only devices that meet the following criteria are allowed to access corporate resources:

- *Smartphones, tablets, and other devices running Android version 2.3 (Gingerbread) and higher.*
- *Smartphones and tablets running iOS 5.0 and higher.*
- *Laptops running Windows 7 and higher*

- *Laptops running Mac OS X Cheetah (10.0) and higher*

The policy applies to any mobile device that is used to access corporate resources, whether the device is owned by the user or by the organization.

The primary goal of this policy is to protect the integrity of the confidential client and business data that resides within THE NEW PAGAN DAWN's technology infrastructure, including internal and external cloud services. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unauthorized resources. A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage the company's public image, breach our data privacy requirements, and violate data privacy laws. Therefore, all employees, contractors, or personnel using a mobile device connected to THE NEW PAGAN DAWN's corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes and policies in doing so.

Applicability

This policy applies to all THE NEW PAGAN DAWN employees, including full and part-time staff, contractors, freelancers, volunteers and other agents who use any mobile device to access, store, backup, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust THE NEW PAGAN DAWN has built with its clients, supply chain partners, and other constituents. Consequently, employment at THE NEW PAGAN DAWN does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

The policy addresses a range of threats to enterprise data, or related to its use, such as:

Threat	**Description**
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive data is deliberately stolen and sold by an employee or unauthorized third party.

Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduc to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of our IT group. Unauthorized use of mobile devices to back up, store, and otherwise access any company-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the company network and resources.

Responsibilities

The TNPD General Secretary of THE NEW PAGAN DAWN has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

The TNPD Tehnic Department of THE NEW PAGAN DAWN has the execution and maintenance of information technology and information systems.

Other staff under the direction of the Board of Directors are responsible for following the procedures and policies within information technology and information systems.

All THE NEW PAGAN DAWN employees, volunteers, contractors, freelancers, agencies and members are responsible to act in accordance with company policies and procedures.

Affected Technology

Connectivity of all mobile devices will be centrally managed by THE NEW PAGAN DAWN's IT department and will use authentication and strong encryption measures. Although IT will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Policy & Appropriate Use

It is the responsibility of any THE NEW PAGAN DAWN employee using a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct THE NEW PAGAN DAWN business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

Access Control

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, and clients at risk.

2. Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by IT. THE NEW PAGAN DAWN will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored at Miradore.com Servers. Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact the helpdesk at tehnic@thenewpagandawn.ei or +40745686833. Although IT currently only allows listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in the future.

3. End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet THE NEW PAGAN DAWN's established enterprise IT security standards.

4. All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected by THE NEW PAGAN DAWN's IT department. Devices that are not approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect. Devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal web address will be

provided to users as required. Smart mobile devices such as smartphones, tablets, and laptops will access the corporate network and data using mobile VPN software installed on the device by IT.

Mobile Device Management (MDM)

1. THE NEW PAGAN DAWN's IT department uses the Miradore mobile device management solution to secure mobile devices and enforce policies remotely. Before connecting a mobile device to corporate resources, the device must be set to be manageable by Miradore.

2. Miradore Online Client's client application must be installed on any mobile devices connecting to corporate resources. Even personal devices owned by employees must have the Miradore Online Client IOS and Android App installed. The application can be installed by contacting the IT department.

3. The mobile device management solution enables IT to take the following actions on mobile devices: [remote wipe, location tracking, remote lock].

4. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all corporate resources, and there may be additional consequences in accordance with THE NEW PAGAN DAWN's overarching security policy.

Security

1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password; a PIN for Mobile Devices or a Password for Desktop/Laptop. All data stored on the device must be encrypted using strong encryption. Employees agree never to disclose their passwords to anyone.

2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.

3. Any non-corporate computers used to synchronize or backup data on mobile devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by THE NEW PAGAN DAWN's IT department.

4. Passwords and other confidential data, as defined by THE NEW PAGAN DAWN's IT department, are not to be stored unencrypted on mobile devices.

5. Any mobile device that is being used to store or access THE NEW PAGAN DAWN data must adhere to the authentication requirements of THE NEW PAGAN DAWN's IT department. In addition, all hardware security configurations must be pre-approved by THE NEW PAGAN DAWN's IT department before any enterprise data-carrying device can be connected to the corporate network.

6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with THE NEW PAGAN DAWN's overarching security policy.

7. Employees, contractors, and temporary staff accessing THE NEW PAGAN DAWN internet resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing company resources of any kind.

8. Employees, contractors, volunteers and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.

9. In the event of a lost or stolen mobile device, the user is required to report the incident to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to company business or personal. The THE NEW PAGAN DAWN Remote Wipe Waiver, which ensures that the user understands that personal data may be erased in the rare event of a security breach, must be agreed to before connecting the device to corporate resources.

10. Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.

11. Usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.

12. Applications that are not approved by IT are not to be used within the workplace or in conjunction with corporate data.

Hardware& Support

1. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

2. Users will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, jail-breaking, rooting) without the express approval of THE NEW PAGAN DAWN's IT department.

3. IT will support the connection of mobile devices to corporate resources. On personally owned devices, IT will not support hardware issues or non-corporate applications.

Organizational Protocol

1. IT can and will establish audit trails, which will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to THE NEW PAGAN DAWN's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with THE NEW PAGAN DAWN's policies.

2. The end user agrees to immediately report to his/her manager and THE NEW PAGAN DAWN's IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.

3. THE NEW PAGAN DAWN [will/will not] reimburse employees if they choose to purchase their own mobile devices. Users [will/will not] be allowed to expense mobile network usage costs.

4. Every mobile device user will be entitled and expected to attend a training session about this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

5. Any questions relating to this policy should be directed to Tehnic Department, at +40745686833or tehnic@thenewpagandawn.eu. A copy of this policy, and related policies and procedures, can be found at Monitorul Pagan Oficial (monitorulpagan.eu).

Policy Non-Compliance

Failure to comply with the *Mobile Device Acceptable Use Policy* may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The Tehnic Department of THE NEW PAGAN DAWN will be advised of breaches of this policy and will be responsible for appropriate remedial action.

Employee Declaration

I, [employee name], have read and understand the above *Mobile Device Acceptable Use Policy*, and consent to adhere to the rules outlined therein.

_____	_____
Employee Signature	Date
_____	_____
	Date
_____	2nd March 2022
IT Administrator Signature	

Mobile Device Remote Wipe Waiver

Purpose

This waiver defines remote wipe technology and ensures that employees understand and agree to its use in the event that a remote wipe is necessary. This waiver is to be read with, and signed in conjunction with the THE NEW PAGAN DAWN Mobile Device Acceptable Use Policy.

The overriding goal of this policy is to protect the integrity of THE NEW PAGAN DAWN data, as outlined in the THE NEW PAGAN DAWN Mobile Device Acceptable Use Policy. Therefore, all users employing a mobile device that connects to THE NEW PAGAN DAWN network, and/or is capable of backing up, storing, or otherwise accessing data of any type, must agree to this remote wipe waiver.

Applicability

This waiver applies to the same devices and users outlined in the THE NEW PAGAN DAWN Mobile Device Acceptable Use Policy. The waiver only applies to devices that are utilized to access THE NEW PAGAN DAWN resources.

Remote Wipe

By connecting to THE NEW PAGAN DAWN technology resources, mobile devices gain the capability of being wiped remotely by THE NEW PAGAN DAWN IT department.

When a remote wipe is initiated by the user or the IT department, the user's mobile device will be wiped of all data and settings. Wiping data, documents, files, settings, and applications in the event a device is lost, stolen, or compromised in any way is critical to protecting our company and its constituents.

If a user requests a remote wipe all data stored on that device will be deleted. A user can later restore personal date from a personal (e.g. from a user's personal computer or from a cloud service to which the user subscribes). It is recommended that users backup their personal data frequently to minimize loss if a remote wipe is necessary.

A remote wipe will only be initiated if IT deems it appropriate. Examples of situations requiring remote wipe include, but are not limited to:

- Device is lost, stolen or believed to be compromised
- Device is found to be non-compliant with company policy
- Device inspection is not granted in accordance with company policy

- Device belongs to a user that no longer has a working relationship with THE NEW PAGAN DAWN.
- The user decides they no longer wish to participate in accordance with Mobile Device Acceptable Use Policy.
- Termination of employment in which the user has not already cleared all THE NEW PAGAN DAWN data by another method approved by IT.

Employee Declaration

I, [employee name], have read and understand the above *Mobile Device Remote Wipe Waiver*, and consent to have my device wiped if the IT department deems it necessary. I further hold THE NEW PAGAN DAWN harmless and absolved of any and all liability that arises from or in connection with remote wipe, remote lock, or remote locate on my personal or provisioned device.

_____	_____
Employee Signature	Date
_____	_____
	Date
_____	2nd March 2022
IT Administrator Signature	

ASOCIAȚIA THE NEW PAGAN DAWN

DEPARTAMENTUL TEHNIC - REGISTRATURĂ

NR DE IEȘIRE. DIT/TNPD/MDM/1/02.03.2022

v. RO

Politica de utilizare acceptabilă a dispozitivelor mobile

Scop

Această politică definește standardele, procedurile și restricțiile pentru toți utilizatorii finali cu utilizări comerciale legitime care conectează dispozitive mobile la rețeaua corporativă, resursele digitale și datele THE NEW PAGAN DAWN. Politica privind dispozitivele mobile se aplică, dar nu se limitează la, toate dispozitivele și mediile însoțitoare care se încadrează în următoarele clasificări:

- *Smartphone-uri*
- *Alte telefoane mobile/celulare*
- *Tablete*
- *Cititoare electronice*
- *Dispozitive media portabile*
- *Dispozitive portabile de jocuri*
- *Calculatoare laptop/notebook/ultrabook*

• *Dispozitive de calcul purtabile*

• *Orice alt dispozitiv mobil capabil să stocheze date corporative și să se conecteze la o rețea*

Pentru a impune securitatea și gestionarea dispozitivelor de la distanță, numai dispozitivele care îndeplinesc următoarele criterii au permisiunea de a accesa resursele corporative:

• *Smartphone-uri, tablete și alte dispozitive care rulează Android versiunea 2.3 (Gingerbread) și o versiune ulterioară.*

• *Smartphone-uri și tablete care rulează iOS 5.0 și versiuni ulterioare.*

• *Laptop-uri care rulează Windows 7 și versiuni ulterioare*

• *Laptop-uri care rulează Mac OS X Cheetah (10.0) și o versiune ulterioară*

Politica se aplică oricărui dispozitiv mobil care este utilizat pentru a accesa resursele corporative, indiferent dacă dispozitivul este deținut de utilizator sau de organizație.

Scopul principal al acestei politici este de a proteja integritatea clientului confidențial și a datelor de afaceri care rezidă în infrastructura tehnologică a THE NEW PAGAN DAWN, inclusiv serviciile cloud interne și externe. Această politică intenționează să împiedice stocarea deliberată sau involuntară a acestor date în mod nesigur pe un dispozitiv mobil sau transportarea într-o rețea nesigură unde ar putea fi accesate de resurse neautorizate. O încălcare de acest tip poate duce la pierderea de informații, deteriorarea aplicațiilor critice, pierderea de venituri, deteriorarea imaginii publice a companiei, încălcarea cerințelor noastre de confidențialitate a datelor și încălcarea legilor privind confidențialitatea datelor. Prin urmare, toți angajații, contractanții sau personalul care utilizează un dispozitiv mobil conectat la rețeaua corporativă a THE NEW PAGAN DAWN și/sau capabil să facă copii de rezervă, să stocheze sau să acceseze în alt mod datele corporative de orice tip, trebuie să adere la procesele și politicile definite de companie. făcând asta.

Aplicabilitate

Această politică se aplică tuturor angajaților THE NEW PAGAN DAWN, inclusiv angajaților cu normă întreagă și parțială, contractanților, liber profesioniști, voluntari și altor agenți care folosesc orice dispozitiv mobil pentru a accesa, stoca, backup sau reloca orice organizație sau date specifice clientului. Un astfel de acces la aceste date confidențiale este un privilegiu, nu un drept, și formează baza încrederii pe care THE

NEW PAGAN DAWN a construit-o cu clienții săi, partenerii lanțului de aprovizionare și alți constituenți. În consecință, angajarea la THE NEW PAGAN DAWN nu garantează automat capacitatea inițială sau continuă de a utiliza aceste dispozitive pentru a obține acces la rețelele și informațiile corporative.

Politica abordează o serie de amenințări la adresa datelor întreprinderii sau legate de utilizarea acestora, cum ar fi:

Amenințare	**Descrierea amenințării**
Pierderea dispozitivului	Dispozitivele folosite pentru a transfera sau transporta fișiere de lucru ar putea fi pierdute sau furate.
Furtul de date	Datele sensibile sunt furate și vândute în mod deliberat de către un angajat sau neautorizat terț.
	Pot fi introduse viruși, troieni, viermi, spyware, malware și alte amenințări către sau prin intermediul unui dispozitiv mobil.
Conformitate	Pierderea sau furtul de date financiare și/sau personale și confidențiale ar putea expune întreprinderea la riscul nerespectării diverselor furturi de identitate și legile privind confidențialitatea.

Adăugarea de noi hardware, software și/sau componente aferente pentru a oferi conectivitate suplimentară pentru dispozitivele mobile va fi gestionată la discreția exclusivă a grupului nostru IT. Utilizarea neautorizată a dispozitivelor mobile pentru a crea copii de rezervă, a stoca și a accesa în alt mod orice date legate de companie este strict interzisă.

Această politică este complementară oricăror politici implementate anterior care se ocupă în mod specific de accesul la date, stocarea datelor, mișcarea datelor și conectivitatea dispozitivelor la orice element al rețelei și resurselor companiei.

Responsabilitati

Secretarul general al THE NEW PAGAN DAWN are responsabilitatea generală pentru confidențialitatea, integritatea și disponibilitatea datelor corporative.

Departamentul Tehnic din THE NEW PAGAN DAWN are in atribuții execuția și întreținerea tehnologiei informației și a sistemelor informaționale.

Alți membri ai personalului aflat sub conducerea Consiliului de Administrație sunt responsabili pentru respectarea procedurilor și politicilor din tehnologia informației și sistemele informaționale.

Toți angajații, contractanții, colaboratorii, membrii și voluntarii THE NEW PAGAN DAWN sunt responsabili să acționeze în conformitate cu politicile și procedurile companiei.

Tehnologia afectată

Conectivitatea tuturor dispozitivelor mobile va fi gestionată central de departamentul IT al THE NEW PAGAN DAWN și va folosi măsuri de autentificare și de criptare puternice. Deși IT nu va gestiona direct dispozitivele personale achiziționate de angajați, se așteaptă ca utilizatorii finali să adere la aceleași protocoale de securitate atunci când sunt conectați la echipamente non-corporate. Nerespectarea acestui lucru va duce la suspendarea imediată a tuturor privilegiilor de acces la rețea, pentru a proteja infrastructura companiei.

Politică și utilizare adecvată

Este responsabilitatea oricărui angajat al THE NEW PAGAN DAWN care utilizează un dispozitiv mobil să acceseze resursele corporative pentru a se asigura că toate protocoalele de securitate utilizate în mod normal în gestionarea datelor pe infrastructura de stocare convențională sunt de asemenea aplicate aici. Este imperativ ca orice dispozitiv mobil care este folosit pentru a desfășura afacerea THE NEW PAGAN DAWN să fie utilizat în mod corespunzător, responsabil și etic. Nerespectarea acestui lucru va duce la suspendarea imediată a contului utilizatorului respectiv. Pe baza acestei cerințe, trebuie respectate următoarele reguli:

Controlul accesului

1. IT își rezervă dreptul de a refuza, prin mijloace fizice și non-fizice, capacitatea de a conecta dispozitive mobile la infrastructura corporativă și conectată la corporație. IT se va angaja într-o astfel de acțiune dacă un astfel de echipament este utilizat într-un mod care pune în pericol sistemele, datele, utilizatorii și clienții companiei.

2. Înainte de utilizarea inițială în rețeaua corporativă sau infrastructura aferentă, toate dispozitivele mobile trebuie să fie aprobate de IT. THE NEW PAGAN DAWN va menține o listă de dispozitive mobile aprobate și aplicații software și utilități aferente și va fi stocată pe serverele Miradore.com. Este posibil ca dispozitivele care nu se află în această listă să nu fie conectate la infrastructura corporativă. Dacă dispozitivul dvs. preferat nu apare pe această listă, contactați biroul de asistență la

tehnic@thenewpagandawn.ei sau +40745686833. Deși IT permite în prezent doar conectarea dispozitivelor enumerate la infrastructura întreprinderii, își rezervă dreptul de a actualiza această listă în viitor.

3. Utilizatorii finali care doresc să conecteze astfel de dispozitive la infrastructura de rețea non-corporativă pentru a avea acces la datele întreprinderii trebuie să utilizeze, pentru dispozitivele lor și infrastructura aferentă, măsurile de securitate considerate necesare de către departamentul IT. Datele întreprinderii nu trebuie accesate pe niciun hardware care nu îndeplinește standardele de securitate IT ale companiei THE NEW PAGAN DAWN.

4. Toate dispozitivele mobile personale care încearcă să se conecteze la rețeaua corporativă prin Internet vor fi inspectate de departamentul IT al THE NEW PAGAN DAWN. Dispozitivele care nu sunt aprobate de IT, nu sunt în conformitate cu politicile de securitate ale IT sau reprezintă orice amenințare la adresa rețelei corporative sau a datelor nu vor avea voie să se conecteze. Dispozitivele pot accesa rețeaua corporativă și datele numai prin Internet folosind o conexiune Secure Socket Layer (SSL) Virtual Private Network (VPN). Adresa web a portalului VPN SSL va fi furnizată utilizatorilor după cum este necesar. Dispozitivele mobile inteligente, cum ar fi smartphone-urile, tabletele și laptopurile vor accesa rețeaua corporativă și datele folosind software-ul VPN mobil instalat pe dispozitiv de IT.

Managementul dispozitivelor mobile (MDM)

1. Departamentul IT al THE NEW PAGAN DAWN utilizează soluția de gestionare a dispozitivelor mobile Miradore pentru a securiza dispozitivele mobile și pentru a aplica politicile de la distanță. Înainte de a conecta un dispozitiv mobil la resursele corporative, dispozitivul trebuie setat să poată fi gestionat de Miradore.

2. Aplicația client Miradore Online Client trebuie să fie instalată pe orice dispozitiv mobil care se conectează la resursele corporative. Chiar și dispozitivele personale deținute de angajați trebuie să aibă instalate aplicația Miradore Online Client IOS și Android. Aplicația poate fi instalată contactând departamentul IT.

3. Soluția de gestionare a dispozitivelor mobile permite IT să întreprindă următoarele acțiuni pe dispozitivele mobile: [ștergere la distanță, urmărire locație, blocare de la distanță].

4. Orice încercare de a încălca sau de a ocoli implementarea managementului dispozitivelor mobile va avea ca rezultat deconectarea imediată de la toate resursele

corporative și pot exista consecințe suplimentare în conformitate cu politica de securitate generală a THE NEW PAGAN DAWN.

Securitate

1. Angajații care utilizează dispozitive mobile și software aferent pentru acces la rețea și la date vor folosi, fără excepție, proceduri securizate de gestionare a datelor. Toate dispozitivele mobile trebuie să fie protejate de o parolă puternică; un PIN pentru dispozitive mobile sau o parolă pentru desktop/laptop. Toate datele stocate pe dispozitiv trebuie criptate folosind criptare puternică. Angajații sunt de acord să nu dezvăluie niciodată parolele nimănui.

2. Toți utilizatorii de dispozitive mobile trebuie să utilizeze măsuri rezonabile de securitate fizică. Se așteaptă ca utilizatorii finali să asigure toate astfel de dispozitive împotriva pierderii sau furtului, indiferent dacă sunt sau nu în uz și/sau transportate.

3. Orice computere non-corporate utilizate pentru sincronizarea sau copierea de rezervă a datelor de pe dispozitivele mobile vor avea instalat software antivirus și anti-malware actualizat, considerat necesar de departamentul IT al THE NEW PAGAN DAWN.

4. Parolele și alte date confidențiale, așa cum sunt definite de departamentul IT al THE NEW PAGAN DAWN, nu trebuie să fie stocate necriptate pe dispozitivele mobile.

5. Orice dispozitiv mobil care este utilizat pentru stocarea sau accesarea datelor THE NEW PAGAN DAWN trebuie să respecte cerințele de autentificare ale departamentului IT al THE NEW PAGAN DAWN. În plus, toate configurațiile de securitate hardware trebuie să fie preaprobate de către departamentul IT al THE NEW PAGAN DAWN înainte ca orice dispozitiv de transport de date al companiei să poată fi conectat la rețeaua corporativă.

6. IT va gestiona centralizat politicile de securitate, rețeaua, aplicația și accesul la date, folosind orice soluții tehnologice pe care le consideră potrivite. Orice încercare de a încălca sau de a ocoli implementarea securității va fi considerată o încercare de intruziune și va fi tratată în conformitate cu politica de securitate generală a THE NEW PAGAN DAWN.

7. Angajații, contractanții și personalul temporar care accesează resursele de internet THE NEW PAGAN DAWN de pe un smartphone sau tabletă NU își vor salva

acreditările de utilizator sau sesiunile de internet atunci când se conectează sau accesează resursele companiei de orice fel.

8. Angajații, contractanții, voluntarii și personalul temporar vor urma toate procedurile de eliminare a datelor aprobate de întreprindere pentru a șterge definitiv datele specifice companiei de pe astfel de dispozitive odată ce utilizarea acestora nu mai este necesară.

9. În cazul pierderii sau furtului unui dispozitiv mobil, utilizatorul este obligat să raporteze imediat incidentul către IT. Dispozitivul va fi șters de la distanță de toate datele și blocat pentru a preveni accesul de către oricine, altul decât IT. Dacă dispozitivul este recuperat, acesta poate fi trimis IT pentru reprovizionare. Ștergerea de la distanță va distruge toate datele de pe dispozitiv, indiferent dacă sunt legate de afacerile companiei sau personale. THE NEW PAGAN DAWN Remote Wipe Waiver, care asigură că utilizatorul înțelege că datele personale pot fi șterse în cazul rar al unei încălcări a securității, trebuie să fie de acord înainte de a conecta dispozitivul la resursele corporative.

10. Utilizarea serviciilor bazate pe locație și a serviciilor mobile de check-in, care utilizează capabilitățile GPS pentru a partaja locația utilizatorului în timp real cu părți externe, este interzisă la locul de muncă.

11. Utilizarea unui dispozitiv mobil pentru a capta imagini, video sau audio, indiferent dacă este nativ pentru dispozitiv sau prin aplicații terțe, este interzisă la locul de muncă.

12. Aplicațiile care nu sunt aprobate de IT nu trebuie utilizate la locul de muncă sau împreună cu datele corporative.

Hardware și suport

1. IT își rezervă dreptul, prin aplicarea politicii și prin orice alte mijloace pe care le consideră necesare, de a limita capacitatea utilizatorilor finali de a transfera date către și de la resurse specifice din rețeaua întreprinderii.

2. Utilizatorii nu vor face modificări hardware sau software care schimbă natura dispozitivului într-un mod semnificativ (de exemplu, înlocuirea sau suprascrierea sistemului de operare, jail-breaking, rooting) fără aprobarea expresă a departamentului IT al THE NEW PAGAN DAWN.

3. IT va sprijini conectarea dispozitivelor mobile la resursele corporative. Pe dispozitivele deținute personal, IT nu va accepta probleme hardware sau aplicații non-corporate.

Protocolul organizatoric

1. IT poate și va stabili piste de audit, care vor fi accesate, publicate și utilizate fără notificare. Astfel de trasee vor putea urmări atașarea unui dispozitiv extern la rețeaua corporativă, iar rapoartele rezultate pot fi utilizate pentru investigarea posibilelor încălcări și/sau utilizări greșite. Utilizatorul final este de acord și acceptă ca accesul și/sau conexiunea sa la rețelele THE NEW PAGAN DAWN să poată fi monitorizate pentru a înregistra datele, orele, durata accesului etc. pentru a identifica modele de utilizare neobișnuite sau alte activități suspecte. Starea dispozitivului, inclusiv locația, adresa IP, numărul de serie, IMEI, poate fi de asemenea monitorizată. Această monitorizare este necesară pentru a identifica conturile/calculatoarele care ar fi putut fi compromise de părți externe sau de utilizatori care nu respectă politicile THE NEW PAGAN DAWN.

2. Utilizatorul final este de acord să raporteze imediat managerului său și departamentului IT al THE NEW PAGAN DAWN orice incident sau incidente suspectate de acces neautorizat la date, pierdere de date și/sau dezvăluire a resurselor companiei, bazelor de date, rețelelor etc.

3. THE NEW PAGAN DAWN [va/nu va] rambursa angajații dacă aleg să-și cumpere propriile dispozitive mobile. Utilizatorilor [vor/nu] li se va permite să cheltuiască costurile de utilizare a rețelei mobile.

4. Fiecare utilizator de dispozitiv mobil va avea dreptul și va participa la o sesiune de instruire despre această politică. Deși unui utilizator de dispozitiv mobil nu i se va acorda acces la resursele corporative folosind un dispozitiv mobil fără a accepta termenii și condițiile acestei politici, angajații au dreptul de a refuza semnarea acestei politici dacă nu înțeleg politica sau nu sunt confortabili cu conținutul acesteia.

5. Orice întrebări legate de această politică trebuie adresate Departamentului Tehnic, la +40745686833sau tehnic@thenewpagandawn.eu. O copie a acestei politici, precum și politicile și procedurile aferente, pot fi găsite la Monitorul Pagan Oficial (monitorulpagan.eu).

Nerespectarea politicii

Nerespectarea Politicii de utilizare acceptabilă a dispozitivelor mobile poate duce, la discreția deplină a organizației, la suspendarea oricăruia sau a tuturor privilegiilor

de utilizare a tehnologiei și de conectivitate, acțiuni disciplinare și, eventual, încetarea angajării.

Departamentul Tehnic al THE NEW PAGAN DAWN va fi imediat informat cu privire la încălcarea acestei politici și va fi responsabil pentru măsurile corective corespunzătoare.

Declarația angajatului

Eu, [numele angajatului], am citit și înțeles Politica de utilizare acceptabilă a dispozitivelor mobile de mai sus și sunt de acord să aderăm la regulile prezentate în aceasta.

_____	_____
Semnătura angajatului	Data
_____	_____
Semnătura managerului	Data
_____	2 martie 2022
Semnătura administratorului IT	

Renunțare la ștergerea de la distanță a dispozitivului mobil

Scop

Această derogare definește tehnologia de ștergere de la distanță și asigură faptul că angajații înțeleg și sunt de acord cu utilizarea acesteia în cazul în care este necesară ștergerea de la distanță. Această derogare trebuie citită și semnată împreună cu Politica de utilizare acceptabilă a dispozitivelor mobile THE NEW PAGAN DAWN.

Scopul primordial al acestei politici este de a proteja integritatea datelor THE NEW PAGAN DAWN, așa cum este subliniat în Politica de utilizare acceptabilă a dispozitivelor mobile THE NEW PAGAN DAWN. Prin urmare, toți utilizatorii care folosesc un dispozitiv mobil care se conectează la rețeaua THE NEW PAGAN DAWN și/sau care este capabil să facă copii de rezervă, să stocheze sau să acceseze în alt mod date de orice tip, trebuie să fie de acord cu această renunțare la ștergere de la distanță.

Aplicabilitate

Această derogare se aplică aceloraşi dispozitive şi utilizatori descrişi în Politica de utilizare acceptabilă a dispozitivelor mobile THE NEW PAGAN DAWN. Renunțarea se aplică numai dispozitivelor care sunt utilizate pentru a accesa resursele THE NEW PAGAN DAWN.

Ștergere de la distanță

Prin conectarea la resursele tehnologice THE NEW PAGAN DAWN, dispozitivele mobile dobândesc capacitatea de a fi șterse de la distanță de către departamentul IT THE NEW PAGAN DAWN.

Atunci când utilizatorul sau departamentul IT inițiază o ștergere de la distanță, dispozitivul mobil al utilizatorului va fi șters de toate datele și setările. Ștergerea datelor, documentelor, fișierelor, setărilor și aplicațiilor în cazul în care un dispozitiv este pierdut, furat sau compromis în vreun fel este esențială pentru protejarea companiei noastre și a constituenților săi.

Dacă un utilizator solicită o ștergere de la distanță, toate datele stocate pe acel dispozitiv vor fi șterse. Ulterior, un utilizator poate restaura data personală dintr-o persoană (de exemplu, de pe computerul personal al unui utilizator sau dintr-un serviciu cloud la care utilizatorul este abonat). Se recomandă ca utilizatorii să facă backup frecvent la datele lor personale pentru a minimiza pierderile dacă este necesară o ștergere de la distanță.

O ștergere de la distanță va fi inițiată numai dacă IT consideră că este necesar. Exemplele de situații care necesită ștergere de la distanță includ, dar nu se limitează la:

• Dispozitivul este pierdut, furat sau considerat a fi compromis

• S-a constatat că dispozitivul nu respectă politica companiei

• Inspecția dispozitivului nu este acordată în conformitate cu politica companiei

• Dispozitivul aparține unui utilizator care nu mai are o relație de lucru cu THE NEW PAGAN DAWN.

• Utilizatorul decide că nu mai dorește să participe în conformitate cu Politica de utilizare acceptabilă a dispozitivelor mobile.

• Încetarea raporturilor de muncă în care utilizatorul nu a șters deja toate datele THE NEW PAGAN DAWN printr-o altă metodă aprobată de IT.

Declarația angajatului

Eu, [numele angajatului], am citit și înțeles Exonerarea de ștergere de la distanță a dispozitivului mobil de mai sus și sunt de acord ca dispozitivul meu să fie șters dacă departamentul IT consideră că este necesar. În plus, îl țin pe THE NEW PAGAN DAWN inofensiv și absolvit de orice răspundere care decurge din sau în legătură cu ștergerea de la distanță, blocarea de la distanță sau localizarea de la distanță pe dispozitivul meu personal sau furnizat.

_____ _____

Semnătura angajatului Data

_____ _____

Data

_____ 2 martie 2022

Semnătura administratorului IT