TUNtex

Mobile Device Acceptable Use Policy

ITP Number ITP-SYS004	**Effective Date** Desember 16, 2005
Category IT Systems Management	**Supersedes** None
Contact itsupport@pttuntex.com	**Scheduled Review** December 2023

Purpose

This security policy establishes rules for the proper use of handheld devices in Tuntex environments in order to protect the confidentiality of sensitive data, the integrity of data and applications, and the availability of services at Tuntex, protecting both handheld devices and users, as well as Tuntex's assets (confidentiality and integrity) and continuity of the Tuntex business (availability).

This mobile device policy applies to all devices and accompanying media that fit the following device classifications:

- Laptop/Notebook
- Tablet computers such as iPads
- Mobile/cellular phone
- Smartphones
- PDAs
- Any mobile device capable of storing District data and connecting to an unmanaged network.

The goal

To protect the integrity and confidential data that resides within Tuntex technology infrastructure. 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 can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss. Therefore, all users employing a mobile device connected to an unmanaged network outside of Tuntex's direct control to backup, store, and otherwise access data of any type must adhere to Tuntex-defined processes for doing so.

Scope

This policy applies to all users: employees, management, consultants, vendors, contractors and others using business or private mobile handheld devices on any premises occupied by Tuntex.

Adherence to these requirements and the security policies derived from them and implementation of provisions is binding across the whole of Tuntex Group, its subsidiaries and majority holdings.

Willful or negligent infringement of the policies of Tuntex and will result in disciplinary, employment, and/or legal sanctions. In the case of the latter the relevant line managers and where applicable legal services shall bear responsibility.

These requirements and the security policies derived from them and implementation provisions also apply to all suppliers of Tuntex. They shall be contractually bound to adhere to the security directives. If a contractual partner is not prepared to adhere to the provisions, he must be bound in writing to assume any resulting consequential damage.

Roles & responsibilities

1. All employees are responsible for adhering to the information security provisions.Specific tasks are documented in the definition of roles.

2. For each role a person must be defined by name and made known to the IT security division.

3. Individuals may assume several roles.

4. Definition of roles applies to all the security policies and implementation provisions derived from this policy.

5. IT security ensures that the roles are documented consistently in corporate quality management.

The following are roles and responsibilities at the management level:

Business owner

- Ensuresthe necessary resources are provided to IT Division

IT governance

Maintains security policies:

- Creation, adaptation to existing policies in place
- Maintenanceup-to-date
- Guidelines and procedures to implement this policy exist and are communicated to the intended people
- Policy and procedures are documented
- Policies and procedures are well communicated
- Is responsible for policy enforcement:
- Ensures that users are properly trained

IT division, IT staff, security administrator, devices manager

- Are responsible of managing mobile handheld devices
- Manage the inventory
- Ensure that the necessary services are available to users
- Provide the necessary resources for the use of services
- Are responsible for policy enforcement:
    - Via the appropriate working controls
    - Make requests for changes/adaptations in this policy to IT governance

Users, Employees

- Must read, understand and agree to security policies
- Must conform to security policies
- Must inform IT staff ofexceptions to security policies

Based on this, 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 Tuntex infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the Tuntex's systems, data, employee, staff and company at risk.

2. Prior to initial use on Tuntex network or related infrastructure, all mobile devices must be registered with IT. Tuntex's IT will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to Tuntex infrastructure. Although IT currently allows only listed devices to be connected to Tuntex infrastructure, it reserves the right to update this list in the future.

3. End users who wish to connect such devices to non-Tuntex network infrastructure to gain access to Tuntex data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT dividion such as updated software, anti-virus software, and personal firewall. Tuntex data is not to be accessed on any hardware that fails to meet TUNTEX's established IT security standards.

   All mobile devices attempting to connect to Tuntex network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by Tuntex's IT division. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to Tuntex network or data will not be allowed to connect. Laptop computers or personal PCs may only access Tuntex network using a Virtual Private Network (VPN) connection.

Security

1. Employees using mobile devices and related software for network and data accesswill, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. Employees agree to never 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 used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain TUNTEX data. Any non-Tuntex computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Tuntex's IT division. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

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

4. Employees, contractors, Full time employee, part time employee and temporary staff will follow all Tuntex-sanctioned data removal procedures to permanently erase Tuntex-specific data from such devices once their use is no longer required.

5. In the event of a lost or stolen mobile device it is incumbent on the user to report this 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.

6. Employees, contractors, Full time employee, part time employee and temporary staff will make no modifications of any kind to Tuntex-owned and installed hardware or software without the approval of the Tuntex Division of Information technology. This includes, but is not limited to, any reconfiguration of the mobile device.

7. Division of Information Technology 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 Tuntex network.

Organizational Protocol

1. Tutex Division of Information Technology can and will establish audit trails and these will be accessed and used without notice. Such trails will be able to track the attachment of an external device to a PC, 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 Tuntex's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Tuntex's highest priority.

Policy Non-Compliance

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

Further information on this policy can be obtained via Tuntex IT Service Desk

Signature_________________________________Annual Review Date __________
By. Dewi update: 1/24/2020