Mobile Device Acceptable Use

Policy Number: IT.IS.08

Effective Date: 8/1/2016

Applicability: New Enterprise Stone & Lime Co., Inc., and its controlled subsidiaries (together "NESL" or the "Company")

Executive Sponsor (ES): Michael Berkley, Chief Information Officer

Document Author: Todd Rist, Information Security & Governance

I. PURPOSE

The purpose of this policy is to define standards, procedures, and restrictions for end users who use the cellular network provided by NESL at the corporate headquarters. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Mobile/cellular phones.
- Laptops/Tablets
- Smartphones.

The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

II. POLICY STATEMENT

This policy applies to all NESL employees, including full and part-time staff, contractors, freelancers, temporary help or other agents who utilize either a company-owned or personally-owned mobile device on NESL property

Such access to this network on site is a privilege, not a right, and NESL does not automatically guarantee the ongoing ability to use these devices to gain access to the cellular network.

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

It is the responsibility of any employee of NESL who uses 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 NESL business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Eligibility

- All exempt employees are eligible to request a company issued smart cell phone. Hourly employees are not eligible for smart cell phones, but their manager can submit an exception request to be issued a Flip-phone. Smartphones are not approved for any hourly employee.

- Hourly employees who receive calls or messages afterhours are required to account for the time they spend handling those calls/messages.

Access Control

- 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 it feels such equipment is being used in a manner that puts NESL's systems, data, users, and customers at risk.

- Prior to initial use on the corporate network or related infrastructure, **all mobile devices must be registered with IT.** NESL will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored on SharePoint under IT Documents. 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 help desk at helpdesk@nesl.com. Although IT currently allows only listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in future.

- **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, **a company-approved personal firewall** and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet NESL's established enterprise IT security standards.

- Whenever possible, NESL issued mobile devices are registered into the Mobile Device Management system, AirWatch and must remain configured in that system at all times.

- All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet or a wireless network) will be inspected using technology centrally managed by NESL's IT department. Devices that have not been previously 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. Laptop computers or personal PCs may only access the corporate network and data 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, PDAs, and UMPCs will access the corporate network and data using Mobile VPN software installed on the device by IT. Please contact the helpdesk at helpdesk@nesl.com if you have any questions.

Security

- **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 or PIN**, and all data stored on the device must be encrypted using **strong encryption**. See the NESL's password policy for additional background. **Employees agree to never disclose or share their passwords with anyone**, particularly to family

members if business work is conducted from home.

- 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 enterprise data. Any non-corporate computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by NESL's IT department. 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.

- Passwords and other confidential data as defined by NESL's IT department are not to be stored unencrypted on mobile devices.

- Any mobile device that is being used to store NESL data must adhere to the authentication requirements of NESL's IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by NESL's IT department before any enterprise data-carrying device can be connected to it.

- 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 NESL's overarching security policy.

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

- 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.

- You will adhere to the policies set by NESL IT and further agree that violation of this requirement may result in a full wipe of your device.

Help & Support

- NESL's IT department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.

- Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of NESL's IT department. This includes, but is not limited to, any reconfiguration of the mobile device.

- 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.

Organizational Protocol

- IT may establish audit trails and these will be accessed, published 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 NESL's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. In all cases, data protection remains NESL's highest priority. Further at its discretion NESL may archive inbound and outbound text message content and phone usage data for eDiscovery purposes.

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

- NESL will not reimburse employees if they choose to purchase their own mobile devices. Users will not be allowed to expense mobile network usage costs as a company supplied mobile device will be supplied to all employees requiring such devices.

    - Every 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.

    - Any questions relating to this policy should be directed to the helpdesk

III. 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 up to and including , termination of employment.

The (i) Vice-President of Finance, (ii) VP of HR (ii) Chief Operating Officer, and (iii) immediate Manager or Director will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.

IV. RESPONSIBILITIES

The Chief Information Officer (CIO) has the overall responsibility for the confidentiality, integrity, and availability of corporate data/network resources.

V. AFFECTED TECHNOLOGY

All mobile devices that connect to, and use cellular services, while onsite at NESL corporate headquarters.

VI. POLICY AND APPROPRIATE USE

It is the responsibility of any employee of NESL who uses a mobile device while onsite at NESL Corporate Headquarters to use their cellular device responsibly. Employees may use their personal cellular devices while on-site, but should do so minimally. It is prohibited during business hours to access non-business related websites/applications such as Facebook, Twitter, YouTube, Amazon.com, gaming sites etc., without prior management approval. It is imperative that any mobile device that is used to conduct NESL business be utilized appropriately, responsibly, and ethically. Failure to do so may result in administrative action up to and including termination.

VII. Help & Support

NESL's IT department will support the company issued hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.

NESL's IT department has no obligation to support non-company issued hardware and software. NESL is not responsible for any issues or damage that may result in the use of the cellular network.

VIII. MONITORING

Individual managers/supervisors are responsible for monitoring their employees' use of cellular services while on-site. It is at the manager's discretion to determine if administrative actions need to be pursued.

IX. WAIVERS

Any deviation, waiver or exception from this policy requires the prior written approval of the Executive Sponsor of this policy, or his or her designee. The Executive Sponsor, or his or her designee, is responsible for tracking all requests for waivers, decisions with respect to those requests, and maintaining documentation related to each waiver request. Each individual receiving a waiver is responsible for retaining documentation of the waiver that he/she was granted.

X. NON-COMPLIANCE

Any employee who violates or circumvents the policy may be subject to disciplinary action up to and including termination.

Next Review By: 30 June 2017

Approval Date: 7 July 2016 Approved By: _____ ___ (Mike Berkley, CIO)

Last Reviewed: 2 June 2016

Appendix

A. Summary of Policies & Procedures Related to [insert Policy Name]

Policy	Policy Areas	Related Procedures
[Insert Policy Name]	[List specific policy areas covered by Policy]	[List any related procedures]

Reviewed By	Version Reviewed	Key Comments/Changes
Todd Rist, IT Security & Governance	Version 1	First attempt at policy revision for discussion purposes.
Mike Berkley, CIO	Version 1	Modified and updated initial version

Names in **bold** have reviewed multiple versions of the document.