 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 1 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

1.0 OVERVIEW

This policy defines the rules regarding the acceptable use of electronic signatures ('e-signatures', 'e-sign/e-signing' or 'digital signatures') as a valid substitute for traditional "wet" signatures within Tutor Perini Corporation and its subsidiaries ('the organization' or 'the company'). Violations of this policy can have a severe audit impact, and thus may lead to revocation of system privileges and/or disciplinary action up to and including termination of employment.

2.0 SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at Tutor Perini Corporation, including all personnel affiliated with third parties. This policy applies to the use of all e-signatures at Tutor Perini Corporation and its subsidiaries, regardless of vendor or method of e-signature, which may be used in a manner that does not conform to the requirements set forth in this policy.

3.0 RESPONSIBILITY


- 3.1. It is the responsibility of all employees, contractors, consultants, temporaries and other workers at Tutor Perini Corporation and its subsidiaries to be familiar with and adhere to this e-Sign Policy. Security and knowledge of the audit requirements set forth in Section 404 of the Sarbanes-Oxley Act of 2002 ('SOX'), as it relates to the e-sign process, is everyone's responsibility. Everyone must understand that they are accountable for e-signatures and requested e-signers at Tutor Perini to comply with this policy.
- 3.2. It is the responsibility of management (Business Unit Controllers or equivalent) and end-users with licensed accounts ('Licensed Users') to enforce compliance with the provisions of this policy on a day-to-day basis.
- 3.3. The Corporate IT Department is responsible for the review and implementation of the provisions of this policy.

4.0 POLICY

- 4.1. **Users are strictly limited to specific, permissible forms of e-signatures for any company-initiated document** – Documents with e-signatures originated by any Tutor Perini company/employee must be created using SignNow. SignNow is the only acceptable platform for company initiated e-signatures. Employees of Tutor Perini and its subsidiaries are not to use any other e-signature platform, including DocuSign and Adobe, for e-signature purposes. Authorized employees may approve documents generated by third parties in other platforms via e-signature.

SignNow is a web application and may be accessed via the SignNow website (<https://app.signnow.com/webapp/login>). Accepted methods of accessing the SignNow website via Egnyte integration, or via document link received at a company email address, are governed by the Procedures.

SignNow is administered and supported by the Corporate IT Department. The SignNow service is delivered and hosted by the 3rd-party vendor Barracuda Networks. SignNow may also be referred to as 'CudaSign' by the vendor.

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 2 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

- 4.2. **Users may only e-sign for themselves and while using their own SignNow account, Active Directory credentials and company email address** – E-signing should be treated the same as applying a “wet ink” signature. Users may only apply e-signatures while representing their own identities—and while using their own unique SignNow accounts—by logging into the SignNow website using their own company email addresses and Active Directory (‘AD’) credentials; or by using document links sent directly to their company email addresses by mail@signnow.com. Under no circumstance is it appropriate to e-sign using another user’s identity, SignNow account or company email address; nor is it appropriate to “spoof” another user’s e-signature within SignNow. SignNow accounts, AD credentials and email addresses may not be shared by users under any circumstance.
- 4.3. **Users may not share passwords** – Passwords are an important aspect of computer security. They are the front line protection for user accounts. A poorly chosen password may result in the compromise of Tutor Perini Corporation’s computer network. As such, users are responsible for taking appropriate steps to select and secure their passwords.


Passwords are to be treated as strictly confidential information. **Employees are responsible for actions taken by others using their disclosed password.** If an account or password is suspected to have been compromised, report the incident to IS Helpdesk and change the password.

- 4.4. **Users may not forward document links to unintended signers and may not e-sign documents when they are not intended signers** – Under no circumstance is it appropriate to forward document links to recipients who are not intended signers, nor e-sign using received document links when the recipient is not an intended signer. Users may e-sign using document links only when received directly from mail@signnow.com.

Users are responsible for any e-sign transactions related to their company email address, including when e-signing via document link not intended for them, or if unintended signers e-sign documents via document link forwarded by the users. Refer to Procedures for further guidance on the appropriate action to take when this situation is encountered.

Instead of forwarding document links, users must reference the below sections and Procedures for accepted methods of re-assigning documents to other users for e-signing while still maintaining an audit trail within SignNow.

- 4.5. **E-signatures must legibly display users’ names as they appear within the company email directory and/or HR records** – Since users are allowed to customize the visual representation of their e-signature when e-signing within SignNow, users must upload or digitally draw a legible visual representation of their name, or choose a legible ‘typed’ version of their name. All e-signatures must be easily matched to an employee name within the company email directory and/or HR records for audit purposes, based solely on the e-signature displayed on the document.
- 4.6. **Users must create a SignNow account using their own company email addresses prior to e-signing documents or initiating documents for e-signing** – The organization classifies two types of end-user accounts based on usage: Free Users and Licensed Users.

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 3 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

Free Users possess accounts intended only for e-signing documents; Free Users do not initiate documents for e-signing – Free User accounts may be created directly by the user via the SignNow website; Free Users must use their company email addresses for account creation. Free Users may only use SignNow under the strict discretion of the Document Owner requesting their e-signatures, Licensed Users, BU Admins (i.e. Business Unit Controller, CFO or VP, further defined in sections below), and under the strict limitations set forth by these Policies and Procedures.

Licensed Users possess accounts intended for e-signing documents, as well as initiating documents for e-signing – (A Licensed User who initiates a document for e-signing is also the Document Owner.) Licensed Users must be approved by BU Admins and can only be created by IT after receiving a formal request via the IT Helpdesk ticketing system. Existing Free Users can be upgraded to Licensed Users only by IT and only after BU Admin approval.

Refer to Procedures for provisioning each type of user.


- 4.7. **User administration is limited to a designated SignNow administrator(s) from the Corporate IT Department ('IT Admin') after receiving approvals from designated administrators at each Business Unit ('BU Admins') via the IT Helpdesk ticketing system** – The organization classifies two types of administrators ('admins') based on usage: IT Admins and BU Admins.

IT Admins are Licensed Users with administrator-level privileges within SignNow, intended for administering and supporting SignNow within the organization – Admin-level access within SignNow (i.e. privileged access) must be approved by the VP of IT. Admin access can only be granted directly by the vendor upon formal request from the VP of IT.

BU Admins are designated employees, typically a Business Unit Vice President, Controller, CFO or equivalent level of management, who approve Licensed Users and manage users at their respective Business Units – BU Admins are designated by the VP of IT upon first approval of SignNow usage at each BU. BU Admins are typically Licensed Users, but may not necessarily possess a SignNow account, so long as BU Admins can perform the functions and responsibilities set forth by these Policies and Procedures.


- 4.8. **All Licensed Users and Free Users are responsible for maintaining an audit trail of all activities within SignNow; and for all e-sign transactions related to their accounts** – Users are responsible for ensuring all transactions can be tied to an individual user's company email and for verifying that transactions associated with the users' own company email addresses are accurate, as follows:

Document Owners are Licensed Users who initiate document for signing, and are responsible for ensuring documents are e-signed properly – Document Owners are responsible for ensuring intended Document Signers (defined below) have Free User or Licensed User accounts prior sending a document for e-signing; verifying e-signatures on

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 4 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

completed documents are legible, match to audit history log, and can be traced to a valid company email address; and maintaining audit trails as follows:

- Document Owners are responsible for ensuring completed documents contain legible e-signatures, time/date stamps and document history audit logs. Document Owners must verify e-signatures legibly display users' names as they appear within the company email directory and/or HR records, as defined in the section above. SignNow automatically places time/date stamps underneath completed e-signature fields; thus, Document Owners must allow adequate space when placing e-signature fields within documents they create, and must verify the time/date stamp is legible. Document history audit logs are provided with the 'document with history' version of completed documents, as defined in the section below.
- If identities and/or audit trail cannot be easily verified on a completed document (i.e. transactions are not tied to an individual company email address), Document Owners are responsible for correcting the document within SignNow and re-sending for corrected e-signatures, or canceling the document and creating a new document with proper e-signatures and audit trails.
- If Document Signers need to be replaced, Document Owners must use the 'Replace Signer' option within SignNow, or cancel and redo the document. Document Owners may also select the "Allow Forwarding" option when creating a document within SignNow, which allows Document Signers to replace themselves as Document Signers while still maintaining audit trails within SignNow. Document links/email notifications should never be forwarded outside of the SignNow application.
- If the same document is sent to multiple Document Signers, with each Signer to be tracked individually with their own copies of the document and individual audit trails (referred to as "Bulk Sending"), the Document Owner must use the 'Bulk Invite' feature within SignNow. The same requirements apply to intended Document Signers being sent Bulk Invites as with individual invites sent via SignNow. It is the Document Owner's responsibility to: ensure each intended Document Signer has a Free User or Licensed User account prior to sending Bulk Invites; and verify 'bulk' documents maintain individual audit trails for each Document Signer, and can be matched to unique individual company email addresses (i.e. no 'Guest' signers or emails entered into text fields with no verification).
- If the Document Owner uses the 'Signing Link' feature within SignNow to create a generic link shared with multiple Document Signers, the Document Owner must enable the option requiring each Document Signer to enter his/her unique company e-mail address (the "Allow signer to send invite" option) and disable 'guest' signing (the "Inviter will guest sign signing step 1" option). The same requirements apply to intended Document Signers being sent Signing Link URLs as with individual invites sent via SignNow. It is the Document Owner's responsibility to: ensure each intended Document Signer has a Free User or Licensed User account prior to sharing Signing Link URLs; and verify documents e-signed via Signing Link maintain individual audit trails for each Document Signer, and can be matched to unique

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 5 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO


individual company email addresses (i.e. no 'Guest' signers or emails entered into text fields with no verification).

- Except for the limited use of 'Signing Link' URLs as strictly defined above, document links/email notifications should never be shared/forwarded outside of the SignNow application. When modifying document workflows and/or sending the same documents to multiple Document Signers, Document Owners must always use available features within SignNow to maintain audit trails for each individual Document Signer. If this cannot be accomplished within SignNow, Document Owners should cancel and redo the documents; and/or initiate a new document workflow for each intended Document Signer individually.
- Document Owners must "flatten" all documents (or print to .pdf) prior to uploading into SignNow. No 'layers' should be used for the final document uploaded for e-signing because of the potential for editing after the document is already complete.

Refer to Procedures for further details on the specific use cases defined above.

Document Signers are Free Users or Licensed Users whose company email is added as an e-signer by a Document Owner – When a document is ready for e-signing, Document Signers receive an email at their company email addresses and a notification within the SignNow website. Document Signers are responsible for verifying they are the intended recipient and for notifying the Document Owner of any document errors. Document Signers are responsible for verifying e-signatures on completed documents are legible, match to audit history log, and can be traced to the e-signer's company email address, as follows:

- To decline to e-sign a document and notify the Document Owner, Document Signers should use the 'Decline to Sign' option within the SignNow document and/or request the Document Owner cancel and redo the document
- If Document Signers wish to replace themselves as Signers (i.e. "forward" the document to a new intended Document Signer while still maintaining audit trails within SignNow), they must use the 'Forward Invite' option within each SignNow document if available. If the 'Forward Invite' option was not enabled by the Document Owner, or for other document workflow modifications, Document Signers should contact the Document Owner to replace them as Signers and/or cancel and redo the document. Document links/email notifications should never be forwarded outside of the SignNow application.
- If Document Signers receive a generic 'Signing Link' URL shared with multiple intended Signers, each Document Signer must enter his/her unique company e-mail address, and must use the individual document link sent to that e-mail address from mail@signnow.com to e-sign the document. If the Document Owner has not enabled these options with the shared Signing Link URL, the Document Signer should not e-sign the document and should contact the Document Owner immediately. Document Signers should ensure that documents e-signed via Signing Link maintain individual audit trails for each Document Signer, and can be matched to unique individual

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 6 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

company email addresses (i.e. no 'Guest' signers or emails entered into text fields with no verification).

- Except for the limited use of 'Signing Link' URLs as strictly defined above, document links/email notifications should never be shared/forwarded outside of the SignNow application. When modifying document workflows and/or forwarding documents, Document Signers must always use available features within SignNow to maintain audit trails for each individual Document Signer. If this cannot be accomplished within SignNow, Document Signers should use the "Decline to Sign" option within the SignNow document and contact the Document Owner, as described above.


Document Signers are also responsible for notifying the Document Owner if identities and/or audit trails cannot be easily verified on completed documents.

Refer to Procedures for further details on the specific use cases defined above.

Document Owners are responsible for retaining copies of documents with e-signature time/date stamps and document history audit logs ('document with history') for audit purposes – If the 'document with history' version of a completed document is not available via automatic email from SignNow or via auto-export to Egnyte, the document with history may be viewed and downloaded directly within the SignNow site.

- 4.9. **All employees must agree to the Company's Acceptable Computer Use Policy which references this e-Sign Policy and Procedures, and therefore all users (Licensed Users and Free Users) are bound by the Policy and Procedures herein; additionally, the 'End-User Agreement Acknowledgment Form' and accompanying User Manual for Licensed Users must be e-signed by each new Licensed User prior to being granted a Licensed account** – IT Admins are responsible for: maintaining the Acceptable Computer Use Policy, ensuring it references this e-Sign Policy and Procedures, and ensuring the most current version is being distributed by HR to new employees; maintaining and administering this e-Sign Policy and 'End-User Agreement Acknowledgement Forms' to Licensed Users prior to granting Licensed User access; and maintaining the e-Sign Procedures, Third-Party Consent Forms, and User Manuals for Licensed Users and Free Users; as outlined below. Completed End-User Agreement Acknowledgment Forms are maintained by IT Admins for audit and internal tracking purposes.

Document Owners are responsible for ensuring intended Document Signers have created SignNow accounts with their company e-mail addresses prior to first e-signing; and understand how to use SignNow, the Policy requirements described herein, and the importance of maintaining an audit trail and preserving their identities (HR administers the Tutor Perini Acceptable Computer Use Policy, which references this e-Sign Policy and Procedures, during the New Hire process) – If an intended Document Signer does not have a Free or Licensed SignNow account, Document Owners are responsible for ensuring the Signer first creates an Free User account (via use of Teams and direct coordination with the Signer, as detailed in the Procedures). It is the responsibility of Document Owners/Licensed Users to: remind new Free Users of their previous and ongoing acceptance of the Acceptable Computer Use Policy and referenced e-Sign Policy and

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 7 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

Procedures, provide link to or copy of the e-Sign Policy and Procedures and User Manual for Free Users, and generally ensure Free Users understand the Policy and audit requirements herein. Document Owners may only send documents for e-signing to Document Signers who have satisfied the above account creation process.


If at any time a Free User is found not to have signed an Acceptable Computer Use Form which specifically references this e-Sign Policy and Procedures, the IT Admin and HR are to be notified immediately – IT Admins should ensure that HR has the employee sign and return the most current version of the Acceptable Computer Use Form, and re-iterate to the Free User that he/she now acknowledges previous, current and future use of e-signatures for company-initiated documents are bound by the e-Sign Policy and Procedures herein. IT Admins should provide a link to or copy of this Policy and Procedures and the User Manual for Free Users.

The e-Sign Policy and Licensed User ‘End-User Agreement Acknowledgment Form’ are distributed within SignNow for e-signing and are maintained by IT Admins prior to provisioning new Licensed User access; completed Forms are retained for audit and internal tracking purposes – Upon receiving an approved request for a new Licensed Account, IT Admins are responsible for ensuring the user first creates a Free User account (via use of Teams and direct coordination with the user, as detailed in the Procedures). Upon the user creating a Free User account, the IT Admin must distribute this e-Sign Policy and End-User Agreement Acknowledgment Form via SignNow for e-signing. Once the Free User e-signs the Form, the IT Admin must verify completeness and accuracy of the e-signed Form. It is the responsibility of IT Admins to retain completed Forms for audit and internal tracking purposes. The IT Admin may make completed Forms available to BU Admins in a centralized location, as needed, at the IT Admin’s discretion. IT Admins may only grant Licensed User access by upgrading Free Users who have completed this process. IT Admins maintain the above documentation, the e-Sign Procedures, Third-Party Consent Forms and the User Manual for Licensed Users; and should provide a link or copies to Licensed Users.

Refer to Attachments below for the ‘End-User Agreement Acknowledgment Form’. Specific procedures are defined within the Procedures document and User Manuals for Free Users and Licensed Users.

If at any time a Licensed User is found not to have signed the End-User Agreement Acknowledgment Form, the IT Admin is to be notified immediately – IT Admins should ensure the most current version of this Policy and the End-User Agreement Form are e-signed by the Licensed User, and re-iterate to the Licensed User that he/she now acknowledges previous, current and future use of the Licensed SignNow account are bound by the e-Sign Policy herein and the Procedures.

This section does not apply to intended Document Signers with email addresses outside of approved company domains (Third-Party Document Signers) – Third-Party Document Signers follow a separate process and require Third-Party Consent Forms, as detailed in the section below.

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 8 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO


- 4.10. **Document Owners must ensure the appropriate ‘Consent Agreement and Acknowledgment Forms’ are signed by intended Document Signers with email addresses outside of approved company domains (Third-Party Document Signers) prior to first e-signing; all Third-Party e-signatures must be completed with two-factor authentication** – Document Owners are responsible for administering Consent Agreement and Acknowledgment Forms to Third-Party Document Signers according to user type, and for retaining users’ responses, prior to users’ first e-signing, as outlined below. Document Owners are responsible for requiring two-factor authentication within SignNow for all documents sent to Third Parties as defined below.

Consent Forms should be e-signed with two-factor authentication within SignNow whenever legally possible; otherwise, Document Owners should retain a completed Form with wet-ink signatures – Refer to Attachments below for each specific ‘Consent Agreement and Acknowledgment Form’.

Document Owners are responsible for ensuring completed Consent Forms are retained as part of the overall final document package for audit purposes – A Consent Form is required for each HR New Hire; or for each Third-Party Signer per original agreement (i.e. subsequent related documents/addendums to the original agreement are generally covered by the initial Consent Form completed for the original agreement). A copy of the completed Forms may be required to be made available to IT Admins and BU Admins in a centralized location for internal tracking purposes, as needed, at the discretion of the IT Admin.

Consent Forms for HR New Hire Employees are distributed by Document Owners (Licensed Users); responses are collected by Document Owners and retained for audit purposes – Document Owners are responsible for distributing the Consent Form to New Hire Employees for e-signing via SignNow using the email address provided to HR; two-factor authentication must be required when sending the document using the New Hire Employee’s provided phone number. Once the user e-signs the Form, the Document Owner must verify completeness and accuracy of the e-signed Form, and retain the completed Form as described above. Document Owners may only send documents for e-signing to New Hire Employees who have completed this process. All documents sent to Third-Party New Hire Employees, including the Consent Forms, require two-factor authentication.

Consent Forms for Third-Party Agreements are distributed by Document Owners (Licensed Users); responses are collected by Document Owners and retained for audit purposes – Document Owners are responsible for distributing the Consent Form to Third-Party Signers. The Third-Party Signer’s company name should be entered in the blank labeled “the Company” within the Consent Form. If possible, Consent Forms should be e-signed via SignNow using the Third-Party Signer’s company email address; two-factor authentication must be required when sending the document using the Third-Party Signer’s provided phone number. The Document Owner must verify completeness and accuracy of signed Forms and retain the completed form as described above. Document Owners may only send documents for e-signing to Third-Party Signers who have completed this process. All documents to Third-Party Signers, including the Consent Forms, require two-

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 9 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

factor authentication using the Signer's email address and phone number.


This section does not apply to employees with existing email addresses within approved company domains (i.e. internal users) – Employees/internal users follow a separate process and do not use Consent Forms; these users are required to use a Free or Licensed SignNow account, and are bound by the Acceptable Computer Use Policy and/or the End-User Agreement, as detailed in the section above.

- 4.11. **All e-sign users are responsible for monitoring their accounts for suspicious or unauthorized activity, and for taking appropriate steps to verify the authenticity of e-sign documents** – All e-sign users acknowledge that when a document is initiated for e-signing within SignNow, an email notification is sent to the company emails of all related Document Owners and Document Signers directly from mail@signnow.com. All e-sign users are responsible for not forwarding emails containing document links to unintended recipients, and for verifying they are the intended recipient of any document link received, as described in further detail within other sections herein.

Suspicious or unauthorized activity should be reported to the Document Owner, BU Admin and IT immediately – Document Signers should decline to e-sign suspicious, incorrect or fraudulent documents (using the 'Decline to Sign' feature within SignNow documents if possible) and must notify the Document Owner immediately, including, but not limited to the following situations: document link received is not directly from mail@signnow.com; users do not appear to be intended recipients/e-signers of the document; and/or email/notification is received indicating that users have signed a document, but have not actually done so.

All e-sign users are responsible for verifying recent completed transactions within their SignNow account via the SignNow website and the available document audit history logs – Users are responsible for reporting unauthorized activity/issues to IT Admins, and for verifying issues are resolved and fully documented for audit purposes. All e-sign users will be responsible for any unauthorized/non-compliant e-sign transactions associated with their company email address if it is determined that the user: received emails/notifications matching suspicious/unauthorized activity as described above, and/or could have identified such activity from the user's document histories; and had a reasonable opportunity to report and correct issues yet failed to do so.

- 4.12. **The Tutor Perini IS Policies and Procedures, which govern general user security and provisioning for IT-supported applications, also apply to the maintenance and administration of the SignNow application** – The SignNow application is subject to IT General Controls and IT SOX audit activities. All user security and provisioning requests, and subsequent resolution, should be retained within the IT Helpdesk ticketing system for audit purposes.
- 4.13. **All e-sign users acknowledge that designated IT Admins from the Corporate IT department have visibility into all user activity, user history, document activity and document history for IT administration and audit purposes; copies of all completed documents are automatically retained in a centralized Egnyte folder for IT Admins.**

 Tutor Perini CORPORATION POLICIES AND PROCEDURES	PAGE 10 OF 10	POLICY NUMBER: IT 3.010
	DATE: 01/31/2017	SUPERSEDES NO: N/A DATED: N/A – Initial Version
SUBJECT: ELECTRONIC SIGNATURE ('E-SIGN') POLICY	ISSUED BY:	APPROVED BY:
DISTRIBUTION: All Tutor Perini Employees	Information Technology Department	TPC VP – IT/CIO

- 4.14. **By using the Tutor Perini SignNow platform, all e-sign users consent to the use of electronic signatures for all records and/or transactions related to each company-initiated document**

5.0 ENFORCEMENT

This policy will be enforced by the Vice President of IT and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company will report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

ATTACHMENTS: 'Consent Agreement and Acknowledgment Forms' For Third-Party Document Signers
 'End-User Agreement and Acknowledgement Form' For Licensed Users

'Consent Agreement and Acknowledgment Forms' For Third-Party Document Signers

a) Consent Form For Third-Party HR New Hires 2017-01-31

b) Consent Form For Third-Party Agreements 2017-01-31



FOR NEW HIRE EMPLOYEES

CONSENT FOR USE OF ELECTRONIC DOCUMENTATION AND ELECTRONIC SIGNATURES (E-SIGNATURES) AGREEMENT AND ACKNOWLEDGMENT FORM

Under the Uniform Electronics Transactions Act (UETA) and the federal U.S. Electronic Signatures in Global and National Commerce Act (E-SIGN Act), the undersigned (I) may be providing certain documents and forms signed in electronic format. By my signature below I agree and acknowledge the following:

I consent to the use of electronic signatures and records in the creation of documents and any subsequent addenda to the documents, if applicable, including, but not limited to New Hire Documents.

I signed or will sign said documents electronically myself, and I acknowledge that I did or may submit said documents electronically via the SignNow e-signature system.

All parties related to these documents, including, but not limited to Human Resources, are authorized to accept and rely on all forms, including: agreements, acknowledgements, disclosures, contracts, and instructions signed and sent electronically through the SignNow e-signature system, for the processing of this New Hire process as if such documents contained my original wet signatures. Said documents so provided shall be fully enforceable and legally binding on the undersigned in the accordance with its terms.

Receiving Paper Copies: I understand that I may request from Tutor Perini (the Company) a paper copy of any record made available electronically to me. I may request delivery of paper copies from the Company by contacting my HR representative directly.

Withdrawing Your Consent: I may decide at any time to receive New Hire documents in paper format from the Company by notifying Human Resources by phone, mail, or electronic means.

Required Hardware and Software: I acknowledge that the following are the hardware and software requirements for access to and retention of electronic records:

Operating Systems: Windows XP or Mac OS X or higher, or iOS 4 or higher

Browsers: Chrome, Firefox, Safari, or Internet Explorer

Email: Access to a valid email account

Phone: Access to a valid phone number to receive SMS/text messages or audio codes for two-factor authentication

Screen Resolution: 800 x 600 minimum

Enabled Security Settings: Allow per session cookies; Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection

Ability to Access Electronic Documents: By completing and sending this consent to the Company, I acknowledge that I can access, e-sign and retain electronic documents.

Signature

Name (Print)

Title

Date



FOR THIRD-PARTY AGREEMENTS

CONSENT FOR USE OF ELECTRONIC DOCUMENTATION AND ELECTRONIC SIGNATURES (E-SIGNATURES) AGREEMENT AND ACKNOWLEDGMENT FORM

Under the Uniform Electronics Transactions Act (UETA) and the federal U.S. Electronic Signatures in Global and National Commerce Act (E-SIGN Act), the undersigned, _____ ("the Company"), may be providing certain documents and forms signed in electronic format. By the Company's signature below the Company agrees and acknowledges the following:

The Company consents to the use of electronic signatures and records in the creation of documents and any subsequent addenda to the documents, if applicable, including, but not limited to: Contract Agreements, Subcontract Agreements, Purchase Orders, Waivers and Releases, Change Orders, and Transmittals.

The Company's authorized representatives signed or will sign said documents electronically, and the Company acknowledges that the Company did or may submit said documents electronically via the SignNow e-signature system.

All parties and third parties to this transaction, including, but not limited to Managers, Contractors, Subcontractors, Architects, are authorized to accept and rely on all contracts, instructions and forms signed and sent electronically through the SignNow e-signature system, for the processing of this transaction as if such documents contained the Company's authorized representatives' original wet signatures. Said documents so provided shall be fully enforceable and legally binding on the undersigned in the accordance with its terms.

Required Hardware and Software: The Company acknowledges that the following are the hardware and software requirements for access to and retention of electronic records: Operating Systems: Windows XP or Mac OS X or higher, or iOS 4 or higher Browsers: Chrome, Firefox, Safari, or Internet Explorer Email: Access to a valid email account Phone: Access to a valid phone number to receive SMS/text messages or audio codes for two-factor authentication Screen Resolution: 800 x 600 minimum Enabled Security Settings: Allow per session cookies; Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection

Ability to Access Electronic Documents: By completing and sending this consent to the other party(ies), the Company acknowledges that the Company can access, e-sign and retain electronic documents.

Signature

Name (Print)

Title

Date

***'End-User Agreement and Acknowledgement Form' For
Licensed Users***

**END-USER AGREEMENT
ACKNOWLEDGEMENT FORM**

I, the undersigned, agree to the terms in the e-Sign Policy, including, but not limited to, the following:

- Users are strictly limited to e-signatures within SignNow for any company initiated document.
- Each user may only e-sign for his/herself and while using his/her own SignNow account, Active Directory credentials and company email address.
- Users may not share passwords.
- Users are responsible for maintaining an audit trail of all activities within SignNow; and for all e-sign transactions related to my account.
- Users may not forward/share document links/email notifications with unintended signers and may not e-sign documents when they are not intended signers.
- I must ensure intended Document Signers have a SignNow account registered to their company email addresses prior to initiating documents for e-signing.
- I am responsible for ensuring completed e-signatures legibly display the Document Signer's name as it appears within the company email directory and/or HR records.
- Since SignNow automatically places time/date stamps underneath completed e-signature fields, I must allow adequate space when placing e-signature fields within documents I create, and must verify the time/date stamp is legible within the completed document.
- I am responsible for ensuring completed documents contain document history audit logs by retaining the full 'document with history' version of completed documents.
- When modifying document workflows and/or sending the same documents to multiple Document Signers, users must always maintain audit trails for each individual Document Signer by using available features within SignNow, including, but not limited to: 'Allow Forwarding', 'Forward Invite', 'Replace Signer', 'Cancel Document Invites', 'Decline to Sign', 'Bulk Sending/Bulk Invite', and 'Signing Link'. If this cannot be accomplished within SignNow, Document Owners should cancel and redo the documents; and/or initiate a new document workflow for each intended Document Signer individually.
- When using the 'Signing Link' feature within SignNow, the option requiring each Document Signer to enter his/her unique company e-mail address (the "Allow signer to send invite" option) must be enabled, and 'guest' signing (the "Inviter will guest sign signing step 1" option) must be disabled.
- I must "flatten" all documents (or print to .pdf) prior to uploading into SignNow. No 'layers' should be used for the final document uploaded.
- I acknowledge that all employees must agree to the Company's Acceptable Computer Use Policy, which references this e-Sign Policy and Procedures; additionally, the e-Sign Policy and 'End-User Agreement Acknowledgment Form' must be e-signed by each new Licensed User prior to being granted a Licensed account and retained for audit purposes.
- I am responsible for monitoring my account for suspicious or unauthorized activity, and taking appropriate steps to verify the authenticity of e-sign documents.
- The appropriate 'Consent Agreement and Acknowledgment Form' must be signed by each Third-Party Document Signer prior to first e-signing and retained for audit purposes; all Third-Party e-signatures, including Consent Forms, must be completed with two-factor authentication.
- I must submit user access/IT requests via the IT Helpdesk ticketing system.

The undersigned has read the Tutor Perini Corporation e-Sign Policy above and understands the



FOR LICENSED USERS

**END-USER AGREEMENT
ACKNOWLEDGEMENT FORM**

policy and procedures described therein. The undersigned agrees to abide by the policy and procedures described therein as a condition of continued employment. The undersigned furthermore understands that violators of this policy and procedures are subject to disciplinary measures including privilege revocation and/or employment termination. The undersigned understands that access to Tutor Perini Corporation information systems and use of e-signatures are privileges which may be changed or revoked at the sole discretion of Tutor Perini Corporation management, and which automatically terminate upon departure from the Company.

The undersigned certifies that he/she has received a copy of the Tutor Perini Corporation e-Sign Policy for future reference, and may also access e-Sign documentation (including, but not limited to: e-Sign Policy, e-Sign Procedures, Third-Party Consent Forms, and the User Manuals for Free and Licensed Users).at any time by visiting: <https://help.tutorperini.com/e-sign-help>

The undersigned also agrees to promptly report all violations or suspected violations of policies and procedures to the SignNow IT Administrator and/or BU Administrator.

Employee Signature

Employee Name (Print)

Date