FORESIGHT

PEOPLE BUILD FASTER WITH AI

WHITEPAPER

Baseline Security Controls

STANDARDS FOR BASELINE CONTROLS

Foresight implements administrative, physical and technical safeguards to protect personal data that are no less rigorous than accepted industry practices, including standards from:

- International Organization for Standardization (ISO): ISO/IEC 27001:2013
- Information Security Management System (ISMS) – Requirements and ISO-IEC 27002:2013, Code of Practice for International Security Management
- Information Technology Library (ITIL) standards
- Control Objectives for Information and related Technology (COBIT) standards
- Or other applicable industry standards for information security

We shall ensure that all such safeguards, including the manner in which personal data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws.

Contents

The following tables define baseline application security controls for protecting personal data, including:

- Application Development
- Session Management
- Vulnerability Management
- Application Logging
- System Hardening
- System Logging
- Password Standards

Control implementation expectations are based on personal data classification.

Application Development

	Control	Status
1	Application development includes reviews for security vulnerabilities throughout the development lifecycle	In place
2	Application change control procedures are documented and followed	In place
3	Controls are in place to protect the integrity of application code	In place
4	Application validates and restricts input, allowing only those data types that are known to be correct	In place
5	Application executes proper error handling so that error messages do not reveal potentially harmful information to unauthorized users (e.g. detailed system information, database structures, etc.)	In place
6	Default and/or supplied credentials are changed or disabled prior to implementation in a staging or production environment	In place
7	Functionality that allows the bypass of security controls is removed or disabled prior to implementation in a staging or production environment	In place

Session Management

	Control	Status
1	Application sessions are uniquely associated with an individual or system	In place
2	Session identifiers are generated in a manner that makes them difficult to guess	In place
3	Session identifiers are regenerated via a change in the access profile of a user or system	In place
4	Active sessions timeout after a period of inactivity	In place

Vulnerability Management

	Control	Status
1	Applications are periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)	In place
2	Application security patches are deployed in a timely manner	In place
3	Procedures for monitoring of new security vulnerabilities are documented and followed	In place
4	Operating system and software security patches are deployed in a timely manner	In place
5	Mitigating controls are deployed for known security vulnerabilities in situations where a security patch is not available	In place
6	System is periodically tested for security vulnerabilities (e.g. vulnerability scanning, penetration testing, etc.)	In place

Application Logging

	Control	Status
1	Successful attempts to access an application are logged	In place
2	Failed attempts to access an application are logged	In place
3	Attempts to execute an administrative command are logged *	In place
4	Changes in access to an application are logged (e.g. adding, modifying or revoking access)	In place
5	Application logs are reviewed on a periodic basis for security events	In place
6	Application logs are protected against tampering	In place

System Hardening

	Control	Status
1	Controls are deployed to protect against unauthorized connections to Services (e.g. firewalls, proxies, access control lists, etc.)	In place
2	Controls are deployed to protect against malicious code execution (e.g. antivirus, antispyware, etc.)	In place
3	Controls deployed to protect against malicious code execution are kept up to date (e.g. software version, signatures, etc.)	In place
4	Intrusion detection and/or prevention software is deployed and monitored	In place
5	Local accounts that are not being utilized are disabled or removed	In place
6	Default supplied credentials (e.g. username and password) are changed prior to implementation	In place
7	Services that are not being utilized are disabled or removed	In place
8	Applications that are not being utilized are removed	In place
9	Active sessions are locked after a period of inactivity	In place
10	Native security mechanisms are enabled to protect against buffer overflows and other memory-based attacks (e.g. address space layout randomization, executable space protection, etc.)	In place

System Logging

	Control	Status
1	Successful attempts to access Information Systems are logged	In place
2	Failed attempts to access Information Systems are logged	In place
3	Attempts to execute an administrative command are logged	In place
4	Changes in access to an Information System are logged	In place
5	Changes to critical system files (e.g. configuration files, executables, etc.) are logged	In place
6	Process accounting is enabled, where available	In place
7	System logs are reviewed on a periodic basis for security events	In place
8	System logs are protected against tampering	In place

Password Standards

The Services also include support single sign-on (SSO) through the industry standard protocols: Security Assertion Markup Language (SAML) v2.

In case the application does not support and enforce SSO, the following controls for Password Security are implemented to comply with the requirements listed in the table below:

Standard Account: An account that does not meet the definitions of Privileged or Service Account below.

Privileged Account: A privileged account is one that runs with elevated privileges; this includes for example administrator and root accounts. They provide access to personal data or sensitive functionality. Sensitive functionality is any functionality which if abused could result in a significant incident or business critical impact.

Service Account: An account type used to provide server/system/process (rather than a person) access to the corporate network for business purposes. Passwords standards for Service Accounts match those of Privileged Accounts except where indicated otherwise with an asterisk (*).

	Security Control	Standard Account	Privileged Account	Comments
Password Complexity				
1	Length	8	15	Widely established standard. Most users should be accustomed to this.
2	Character Set	2 classes (including one non-alphabetical, upper and lowercase alphanumerical characters)	3 classes (at least 1 capital letter, lower-case letter, number, and non-alphanumeric character)	Prevents simple dictionary words and forces an increased character set for brute forcing.
Password Changing				
3	Forced Change	Required on initial account set up, and after any automated or helpdesk password reset	Required on initial account set up, and after any automated or helpdesk password reset	This prevents technical support staff from knowing an application user's password.
4	Old Password Entry	Entered prior to password change (except where forced)	Entered prior to password change (except where forced)	Forced password change will occur immediately after password entry, so there is no need to ask again.
Account and Password Aging				
5	Maximum Age	90-180 days	90-180 days	It is recommended that users are provided with advice and the date of the last password change.
6	Minimum Age	1 day	1 day	Set to one to allow accounts to be changed after one day.
7	Password History	None	12 changes or two years, whichever is greater	**Standard Account -** Not relevant if no password maximum age is enforced. **Privileged Account –** 12 changes ensure the same password cannot be re-used within at least a 2-year time period.
8	Account Expiry	Shared Accounts / Time limited accounts	<=90 days	Any shared or time limited accounts such as demo accounts on products must be set to expire after a predetermined time period (e.g., 3 months).

	Security Control	Standard Account	Privileged Account	Comments
9	Account Inactivity	>90 days	>90 days	This prevents inactive users with illegitimate reasons (e.g. terminated employee) from signing onto an account.
Password Lockout				
10	Lock Out Attempts	5 attempts	5 attempts	**Standard Account -** This allows the user to try to correct suspected mistyping, CAPS LOCK etc., and try several different password possibilities. **Privileged Account -** This protects a privileged account from being brute force attacked by ensuring it becomes inactive when suspected of misuse.
11	Lock Out Duration	30 hours	Permanent, until reset	**Standard Account -** Limits failed login attempts to 10 per hour. Note that password may be reset during lock out period. **Privileged Account –** This ensures adequate oversight of the reactivation process when a suspected brute force attack has occurred.
Password Storage, Transmission and Display				
12	Storage	Salted Hashed (preferred) or Reversible Encryption	Salted Hashed (preferred) or Reversible Encryption	See the Cryptographic Algorithm Standard for specific requirements and recommended implementations.
13	Transmission	Encrypted across all networks	Encrypted across all networks	Encrypted sessions should be used (e.g. SSL) for all login screens. This also allows authentication of the server.
14	Caching	Allowed (with global disable)	Not Allowed	**Standard Account -** If password caching is used the cookie should be held and transmitted securely. **Privileged Account –** Password caching should be disabled to prevent unauthorized use.
15	Display	Masked character by character	Masked character by character	Password entry screens should always mask the input characters. This is standard industry practice.

	Security Control	Standard Account	Privileged Account	Comments
Forgotten Password				
16	Reset/Remind	Reset Only	Reset Only	Users should never be told their password, as this risks compromising other accounts if they happen to use the same password. Hashed storage would prevent Customer from recovering the password.
17	Reset Value	Randomly (computer) generated according to complexity/length	Randomly (computer) generated according to complexity/length	The new password must not be predictable or guessable. It must not be the same for every user, nor the same for every password reset by a particular user.
Session Management				
18	Inactivity timeout	Optional, based on business needs	15 minutes	**Standard Account –** Inactivity timeouts should be enabled unless they need to operate for prolonged periods without user interaction (e.g. backup accounts) **Privileged Account –** Sessions should be discontinued after 15 minutes of inactivity to protect them from unauthorized use.
19	Maximum session time	Optional, based on business needs	18 hours*	**Standard Account** - Sessions should be limited to some period of time corresponding to a normal maximum working period for the user (e.g. 18 hours). **Privileged Account** – Sessions should be defined to a maximum of 18 hours and require re-authentication to continue past that period. *For Service Accounts this value is optional based on business needs as session needs may vary by product and service. Where a service will take longer than 18 hours to complete (e.g. backup services) the value should be set to the expected completion time. Otherwise, this value should match that of Privileged Accounts.

	Security Control	Standard Account	Privileged Account	Comments
Session Management				
20	Concurrent Log In	Prevented	Prevented	Concurrent logins or other forms of account sharing should be prevented, or, where this is not possible, procedures must be in place to detect, report and investigate potential attempts at concurrent login or sharing (e.g., excessive numbers of logins, simultaneous logins from different locations etc.).

About Foresight

Foresight's construction project management platform helps owners and contractors deliver major projects on-time and on-budget by automatically identifying priorities, risks, and action plans in Primavera P6 or Microsoft Project schedules. We place the schedule at the heart of project execution, enabling project managers, controllers and schedulers to make data-driven decisions. Leveraging AI, machine learning and natural language processing, Foresight unleashes predictive insights about delay risks and work prioritization. Our secure, scalable and user-friendly platform revolutionizes your planning and execution by creating proactive 'look-ahead' action plans, igniting dynamic collaboration, staying head of risks, learning from past projects, and enhancing schedule visibility/reporting.

Contact us to learn more

www.foresight.works