Policies and Standard

Information Security Framework: Cyber Security Standard

Version: 1.6

Release date: 2019-12-30

Document classification: PUBLIC

FORESIGHT® CYBER

CONTENTS

INTRODUCTION

This document expands upon policy statements within the Foresight Cyber Information Security Policy, documenting detailed configuration standards to be implemented.

SYSTEM CRITICALITY AND SECURITY CONTROLS

For low-impact information systems, as a minimum, employ appropriately tailored security controls from the low baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

Critical systems: Any Foresight Cyber system accessible from the Internet, Cloud production systems, PCs used in development of Foresight Cyber critical applications, any system used to store and process customer data, any system used to store and process privacy related information.

The list of critical systems is maintained on-line and replicated into the Appendix E.

Non-critical systems: other office PCs, printers

Exceptions to this classification can be authorised by CTO pending sound technical and business justification. All exceptions must be recorded in the change ticketing system.

SYSTEM SECURITY

The head of Technology Operations is responsible for correct implementation of the following requirements.

Vulnerabilities and security patches

Vulnerabilities are prevalent in all ICT environments. These vulnerabilities are often exploited by malicious actors in order to gain access to information assets. As such, rectifying weaknesses within Foresight Cyber IT systems is crucial to maintaining a continued business operation. However, not all vulnerabilities are equivalent, requiring remediation specifically related to the current threat, the likelihood of exploitation and the criticality of systems to business risk.

As such, it is responsibility of Foresight Cyber IT to monitor emerging vulnerability & threat intelligence and obtain information about active vulnerabilities present in Foresight Cyber systems.

The following timelines should be adopted as a remediation standard:

Vulnerability criticality [1]	Internet facing systems	Critical systems	Non-critical systems
5	Fix in 24 hours	Fix in 7 days	Fix in 30 days
4	Fix in 48 hours	Fix in 14 days	Fix in 40 days
3	Fix in 30 days	Fix in 30 days	Fix in 90 days
1-2	Fix as part of normal software updates		

If a vulnerability cannot be fixed, mitigating controls such as additional monitoring, should be established to monitor, and alert, any attempts to exploit the vulnerability of Foresight Cyber systems.

System Hardening

All Foresight Cyber systems should be hardened to manufacturers or industry best practices appropriate for systems criticality, especially:

- Only required software should be installed and active.
- The baselines should be modified to enforce password and account lockout policy as above.
- All accounts used for non-admin work must not be set as administrators on respective systems.
- The use of Centrum for Internet Security (CIS) benchmarks is recommended. https://learn.cisecurity.org/benchmarks
    - Internet facing and critical systems – hardened to Level 2
    - All other systems hardened to Level 1 at minimum

[1] **Note:** When, as part of threat intelligence feed, a vulnerability is reported to be 'Part of exploit kit', or 'Actively exploited' then the vulnerability should be considered as having a criticality rating of 5 and corrected in line with the ratings shown.

SYSTEM ACCESS SECURITY

The head of Technology Operations is responsible for correct implementation of the following requirements.

General Account Settings

Accounts should:

- Only be created for use by an individual for Business as Usual (BAU) activities.
- Not be shared (used by multiple persons) unless approved with a valid business justification

Password settings

Passwords for all accounts, MUST be at least 12 characters or longer, and:

- Have a mix of upper case, lower case, symbols, and numbers; and contain at least three of those four groups.
- Not be a common word or phrase
- Not contain a date, a name, or other things that can be associated with you.
- Not be reused or shared across multiple accounts, whether personal or corporate
- Not be shared with anyone inside or outside Foresight Cyber
- Use a password manager or safe where practicable [2]

Passwords should be changed when:

- A suspected or confirmed breach occurs
- A person leaves Foresight Cyber, even if the account is disabled
- A shared password known to multiple people when one or more of these no longer require access

[2] Foresight Cyber standard password manager is 1Password and users can sign-up via Teams

Foresight Cyber systems should be set up to enforce these rules where technically feasible.

Privileged password step-up

In addition to the previous requirements, privileged accounts, such as administration accounts, MUST

- Have a minimum password length of at least 16 characters
- Have passwords changed every 180 days
- Prevent the re-use of the previous 24 passwords
- Reviewed at least annually and disabled if no longer required

Multi-factor security

All accounts, where technically and commercially feasible, should be enabled to enforce multi-factor authentication. The supported multi-factors are listed in NIST SP800-63b however the use of SMS based MFA is discouraged for user accounts and MUST NOT be used for admin accounts.

The authorised MFA methods are:

1. Yubikey using OTP, FIDO2 or Smart Card configurations
2. Microsoft Authenticator (in the decreasing order of preference):
    a. Managed Identity for password less login
    b. Managed identity setup to prompt users to Approve / Deny requests
    c. Standard TOTP – time-based code
3. A smart card with an approved private key using approved crypto methods

Please note: A text message sent over a GSM network is considered weak authentication and should be only used as an exception if above methods are not possible to setup.

Account protection

When a system allows, account usage should be monitored for successful and unsuccessful login attempts. When 8 unsuccessful login attempts are detected in a 30 minute timeframe, the account should be frozen for at least 15 minutes and an alert reported to security operations.

LOGGING & ANALYSIS

The head of Technology Operations is responsible for correct implementation of the following requirements.

Systems should be set to log at very minimum:

- Login attempts – success and failure
- Logout events - success
- Any account and group management operations
- Object access – set for critical objects
- Password changes – success and failure
- Any changes in privilege associations, e.g. an amendment to permissions

Logs should be retained for at least 30 days on originating devices, or sent to centralised log collection for long-term storage and analysis.

CRYPTOGRAPHY

The head of Technology Operations is responsible for correct implementation of the following requirements.

Only industry standard crypto functions and modules should be used. The following parameters should be used as a baseline for setting cryptography parameters:

- Use at least 128b key length for symmetric cryptography, but optimally 256b
- Use at least 128b effective equivalent symmetric strength for asymmetric cryptography using elliptic curves, i.e. means 2x more bits than symmetric ciphers
- Use at least 2048b effective strength for asymmetric cryptography when not using elliptic curves
- Use at least 2048b effective strength for asymmetric cryptography Diffie-Helman key exchange, but optimally Elliptic curves
- Use SHA2 or stronger hashing standard

For password storage, prefer **scrypt**, **bcrypt** and **Password-Based Key Derivation Function 2** in the descending order of preference

Where possible and required, hardware-based key generation & protection should be utilised – e.g. TPM chip, Chip card, Amazon CloudHSM (https://aws.amazon.com/cloudhsm/)

Appendix A details IPSec and OpenVPN settings.

Appendix B details TLS servers and client settings.

INCIDENT DETECTION AND RESPONSE

The head of Technology Operations is responsible for correct implementation of the following requirements.

Foresight Cyber systems must be setup, as per this standard, to log actionable messages into centralised log management system. Foresight Cyber managed systems that are delivered as part of client services should log locally or to client's log management system.

The following possible triggers should be properly managed as part of the incident response process:

1. Externally received vulnerability / breach disclosure
2. Internally discovered cyber security incident

As each incident is typically a various combination of factors, it is impossible to put a complete procedure into the place. However, there must be a place to document incident playbooks [3]as these are agreed, either based on best practices or past incidents (lessons learned).

Each playbook should also contain non-technical elements, such as Public relations, legal implications, etc.

[3] An example of playbooks can be obtained here: https://www.incidentresponse.com/playbooks/

DISASTER RECOVERY

Foresight Cyber, being an agile company, is determined to recover from disasters of various kind that would threaten its capability to survive.

It is the responsibility of the CEO to ensure that the company has actionable, sound and communicated plans covering pre-determined disasters.

RELATED DOCUMENTS

- Foresight Cyber Information Security Policy
- NIST SP800-77, Guide to IPSec VPNs, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf
- NIST SP800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
- Deploying Strong DH, https://weakdh.org/sysadmin.html
- NIST IR-7966, Security of Interactive and Automated Access Management Using Secure Shell (SSH), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7966.pdf

Revision History

Version	Revision Date	Description
1.0	2017-05-01	First version
1.1	2017-09-02	Updated crypto section
1.2	2017-10-09	System criticality and IAM levels
1.3	2018-08-23	OpenVPN, TLS changes
1.4	2018-06-10	TLS changes
1.5	2019-10-15	Clarifications of responsibilities Added sections for Incident response and Disaster recovery
1.6	2019-12-30	Changes to ciphers – removed CBC encryption algorithms

APPENDICES

Appendix A: IPSec VPN and OpenVPN settings

These settings are a recommended minimum to satisfy current security threats. We reference NIST IPSec guide SP800-77 and

IPSec VPN and OpenVPN connections should be used for:

- Gateway-to-gateway. This model protects communications between two specific networks, such as an organisation's main office network and a branch office network, or two business partners' networks.
- Host-to-gateway. This model protects communications between one or more individual hosts and a specific network belonging to an organization. The host-to-gateway model is most often used to allow hosts on unsecured networks, such as traveling employees and telecommuters, to gain access to internal organizational services, such as the organisation's e-mail and Web servers.

Host to host connection that require integrity and confidentiality protection should use TLS connection – see Appendix B. In exceptional cases IPSec AH protocol can be used for host to host connections.

IPSec

Phase 1 – IKE Security Association

Parameters	Minimum Settings	Note
IKE version	V2	V1 may be used when V2 is not supported by the peer
Authentication	Pre-shared key of 128 bits strength	Unique for each IKE SA
Encryption	AES 128 bits CBC	
Hash	SHA2	SHA1 may be used when stronger has is not supported by the peer
DH Group	14 (2048 bits)	DH5 group may be used when stronger has is not supported by the peer
Lifetime	86400 seconds (24 hours)	

Phase 2 – Child Security Association

Parameters	Minimum Settings	Note
Encryption	AES 128 bits CBC, AES128-GCM (128 bits)	
Hash	SHA256, AES-XCBC	SHA1 may be used when stronger has is not compatible on the peer
PFS group	14 (2048 bits)	PFS can be disabled is it is incompatible with the other party VPN end points
Lifetime	28800 seconds (8 hours)	

OpenVPN

Cryptographic settings

Parameters	Minimum Settings	Note
TLS authentication	Enabled	
Encryption	AES 128 bits CBC	Optimal: Ciphers AES-256-GCM
Auth digest algorithm	SHA256, AES-XCBC	SHA1 may be used when stronger hash is not compatible on the peer
DH Group	14 (2048 bits)	Optimal: ECHD Only, Default curve
Strict User-CN Matching	Yes	
NCP Algorithms	AES-256-GCM	
Enable NCP	Yes	
TLS Key Usage Mode	Encryption	Optimal: Encryption + Authentication

1. Admin VPN

Additional settings over User VPNs:

Parameters	Minimum Settings	Note
Inter-client communication	Disabled	
Topology	/30 isolated clients	
Fixed IPs	Yes	

Appendix B: TLS Connections requirements

As per NIST SP800-52, the TLS connections should be secured as below.

1. Testing of configuration

All web servers must achieve, at minimum, grade A on https://www.ssllabs.com. In addition, the test must show:

Test	Value
Issuer	Let's encrypt or DigiCert
Weak key (Debian)	No
Revocation status	Good
Trusted	Yes
DROWN	No
Secure Renegotiation	Supported
BEAST attack	Mitigated-server side
POODLE (SSLv3)	No
POODLE (TLS)	No
Heartbleed (vulnerability)	No
Ticketbleed (vulnerability)	No
OpenSSL CCS vuln. (CVE-2014-0224)	No
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No
Forward Secrecy	Strong
Uses common DH primes	No[4]
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
RC4	Not supported

2. Protocol Version Support

All TLS versions above 1.2 MUST be enabled, and where possible the latest TLS version SHOULD be used by default and as a sole protocol.

3. Server Keys and Certificates

The TLS server shall be configured with one or more public key certificates and the associated private keys. TLS server implementations should support multiple server certificates with their associated private keys to support algorithm and key size agility.

[4] https://weakdh.org/sysadmin.html

At a minimum, the server shall be configured with ECDSA signature certificate using a SuiteB (P-256 and P-384) named curve for the signature and public key in the ECDSA certificate should be used.

The email servers should in addition be configured with an RSA key encipherment certificate, and also should be configured with an ECDSA signature certificate or RSA signature certificate.

TLS servers shall be configured with certificates issued by a CA, rather than self-signed certificates. Furthermore, TLS server certificates shall be issued by a CA that publishes revocation information in either a Certificate Revocation List (CRL) [RFC5280] or in Online Certificate Status Protocol (OCSP) [RFC6960] responses. The source for the revocation information shall be included in the CA-issued certificate in the appropriate extension to promote interoperability.

4. Cipher Suites

The server shall be configured to only support cipher suites for which it has a valid certificate containing a signature providing at least 128 bits of security. All TLS servers MUST be limited to strongest ciphers compatible with TLS 1.2 and above, using ECDHE. The DHE ciphers should be avoided due to weak 1024 DH key size. The CBC encryption should be avoided due to lower security.

Acceptable cipher suites for a TLS server that has been configured with an RSA private key and a corresponding RSA certificate:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

ECDHE Server Certificates cipher suites that may be supported by a server that has been configured with an elliptic curve private key and a corresponding ECDH certificate signed using ECDSA:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

DSA Server Certificates cipher suites that may be supported by a server that has been configured with a DSA private key and a corresponding DSA certificate:

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

DH Server Certificates cipher suites that may be supported by a TLS server that has been configured with a DH private key and a corresponding DH certificate signed using DSA:

- TLS_DH_DSS_WITH_AES_128_GCM_SHA256
- TLS_DH_DSS_WITH_AES_256_GCM_SHA384

5. Discouraged TLS Extensions

- Client Certificate URL - The Client Certificate URL extension allows a client to send a URL pointing to a certificate, rather than sending a certificate to the server during mutual authentication. This can be very useful for mutual authentication with constrained clients. However, this extension can be used for malicious purposes.

6. Client Authentication

Where strong cryptographic client authentication is required, TLS servers may use the TLS protocol client authentication option to request a client certificate to cryptographically authenticate the client. All TLS servers that perform client authentication shall support certificate-based client authentication.

The TLS server shall be configurable to terminate the connection with a fatal "handshake failure" alert when a client certificate is requested, and the client does not have a suitable certificate.

Appendix C: SSH Connections requirements

The strength of the crypto settings for SSH must be at least the equal to the TLS connections.

Authentication to SSH servers MUST ONLY be performed using SSH user keys. The below configuration file details mandated settings:

```
Port 2222
Protocol 2
#HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
Ciphers chacha20-poly1305@openssh.com,aes256-ctr
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org
MACs hmac-sha2-512,hmac-sha2-256,hmac-sha2-256-etm@openssh.com
RekeyLimit 1G
SyslogFacility AUTH
```

```
LogLevel DEBUG
LoginGraceTime 1m
PermitRootLogin no
StrictModes yes
MaxAuthTries 6
MaxSessions 10
PubkeyAuthentication yes
HostbasedAuthentication no
IgnoreRhosts yes
PasswordAuthentication no
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM no
AllowAgentForwarding no
AllowUsers vj lm
AllowTcpForwarding yes
X11Forwarding no
PrintMotd no
UsePrivilegeSeparation sandbox
UseDNS yes
AcceptEnv LANG LC_*
Subsystem   sftp   /usr/lib/openssh/sftp-server
```

Appendix D: Identity and Access Security levels

1. Identity Assurance Level

IAL1: At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.

IAL2: At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in SP 800-63A.

IAL3: At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation as described in SP 800-63A.

2. Authenticator Assurance Level

AAL1: AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.

AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.

AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a "hard" cryptographic authenticator that provides verifier impersonation resistance.

Appendix E – Critical systems

The following systems have been categorised as business critical. The list is replicated from Teams Wiki which also contains detailed information for each system.

- Office 365 & AzureAD
- Request Tracker – support.foresightcyber.com
- Zabbix
- Elastic Stack
- Windows 10 used by users assigned client roles
- Linux Debian used on systems running critical applications and used for any client production service
- PFSense Firewall

Foresight Cyber Ltd

Registered address:
International House, 24 Holborn Viaduct,
City of London, London, EC1A 2BN,
United Kingdom

Business address UK :
Universal House, Suite 3,56-58 Clarence Street,
Kingston upon Thames, KT1 1NP,
United Kingdom

Business address CZ:
Fryštátská 64/9, 733 01 Karvina,
Czech Republic

Contacts:
UK Office: +44 20 7183 9858
General enquiries: info@foresightcyber.com
Finance team: finance@foresightcyber.com
Data protection Office: dpo@foresightcyber.com
Directors: directors@foresightcyber.com

https://foresightcyber.com
@foresightcyber.com

VAT: GB144735213
Company number: 06871193
D-U-N-S number: 211601017

OUR CERTIFICATIONS