Custom Created DFARS Compliant Policy Suite

Thank you for purchasing the Continuum GRC Policy Machine policy suite. Please answer all the following questions completely. Once this is completed and your questionnaire is submitted, you will be able to download your policy suite under the My Documents tab.

Should you require any assistance with this process please call 1-888-896-6207.

Identification and Preamble

What is the Company's name? *

What is the Company's DBA name? *

What is the Company's location of incorporation? *

What is the Company's primary business address? *

Street Address

Address Line 2

City

State / Province / Region

Postal / Zip Code

Country

What is today's date?

/ MM / DD YYYY

What is the date that these policies were originally drafted on? *

/ MM / DD YYYY

What is the date that these policies were originally ratified on? *

/ MM / DD YYYY

What is the date of the most recent version of this policy? *

/ MM / DD YYYY

When will the next document recertification date be?

9 / MM 5 / DD 2019 YYYY

How would you like to identify the policy version going forward? *

Who was the original author of this document? *

First Last

Who is responsible for authorizing the implementation of this policy? *

Governance Controls

How often does the Company's change advisory board meet? *

- Daily
- Weekly
- Monthly
- Quarterly
- Annually
- Ad-Hoc

What governance framework do you rely on for certification or guidance? *

- ISO 27001
- COBIT
- COSO
- ITIL
- PCI
- FISMA

Choose the appropriate response. *

- the Company is required to maintain certifications and or regulatory requirements
- the Company is not required to maintain certifications or regulatory requirements

Does the company comply with any industry certifications or regulatory mandates? *

- not applicable
- ISO 27001 -
- FedRAMP -
- COSO -
- HIPAA -
- PCI -

- [ ] CJIS -
- [ ] DFARS -
- [ ] AICPA SOC 1 -
- [ ] AICPA SOC 2 -
- [ ] GDPR -
- [ ] NERC CIP -
- [ ] Other

Audit logs must be retained on-line for a time period defined by a Document Retention Schedule or otherwise defined by legal requirements which currently is: *

- ( ) 30 days (1 month)
- ( ) 90 days (3 months)
- ( ) 180 days (6 months)
- ( ) 365 days (12 months)
- ( ) 395 days (13 months)
- ( ) Other

Each system will provide sufficient storage to ensure logs will not be overwritten during normal operating conditions. *

- ( ) 50%
- ( ) 100%
- ( ) 200%
- ( ) 300%
- ( ) Other

Technical Controls

Password length must be how many characters or longer? *

- ( ) six (6)
- ( ) eight (8)
- ( ) ten (10)
- ( ) Other

Password length must contain at least how many alphabetic characters? *

- ( ) one (1)
- ( )

- two (2)
- three (3)
- Other

Grace log-ins after a required password change are limited to how many log-ins? *

- one (1)
- two (2)
- three (3)
- Other

Password length must contain at least how many non-alphabetic characters? *

- one (1)
- two (2)
- three (3)
- Other

What is the number of days before password changes are required? *

- 30 Days
- 60 Days
- 90 Days
- Other

What is the number of days before accounts are deleted from the system? *

- 30 Days
- 60 Days
- 90 Days
- Other

What is the number of days before accounts are disabled for inactivity? *

- 6 Days
- 15 Days
- Other

What is the number of days prior to account password expiration are users notified? *

- ○ 5 Days
- ○ 10 Days
- ○ 15 Days
- ○ Other

What is the number of failed log-on attempts before disabling the user ID? *

- ○ one (1)
- ○ two (2)
- ○ three (3)
- ○ Other

Idle sessions should be disconnected after: *

- ○ fifteen (15) minutes
- ○ twenty (20) minutes
- ○ eight (8) hours
- ○ twenty-four (24) hours
- ○ Other

What is the Company approved public-key algorithm key strength? *

- ○ 1024 bit
- ○ 2048 bit
- ○ Other

What is the Company's work order or ticketing system called? *

Administrative Controls

What is the name of the person who is responsible for maintaining these policies in general? *

First Last

What is the title of the person who will maintain these document going forward? *

What is the contact number for the information security group or person responsible for enforcing these policies? *

What is the name of the person within the organization that supervises the person who is responsible for these policies in general? *

First Last

What is the title of the person within the organization that supervises the person who is responsible for these policies in general? *

What is the title of the person who is responsible for maintaining these policies in general? *

What is the title of the person who oversees business administrative operations in general? *

Incident Response and Business Continuity Controls

Who is the person responsible for your organizations Security Incident Response Team (SIRT) or person with a similar role? *

First Last

What is your Security Incident Response Team (SIRT) contact number? *

What is the email address for the person responsible for your organizations Security Incident Response Team (SIRT) or person with a similar role? *

What is your Physical Security Team contact number? *

Privacy and Classification Controls

The use of document sharing/syncing applications (e.g. DropBox or Box.net) *

- ○ are not permitted
- ○ are permitted

The use of native cloud syncing solutions (e.g., iCloud, SkyDrive, Google Drive) *

- ○ are not permitted
- ○ are permitted

All Company information shall be classified in one of four confidentiality categories which are:
• Restricted • Confidential • Internal Use Only • Public

As it relates to Restricted information classifications, the the unauthorized disclosure of which would to what to the Company? *

(Insert company-specific examples)

As it relates to Restricted information classifications, what are Company examples? *

(Insert company-specific examples)

As it relates to Confidential information classifications, the the unauthorized disclosure of which would to what to the Company? *

(Insert company-specific examples)

As it relates to Confidential information classifications, what are Company examples? *

(Insert company-specific examples)

As it relates to Internal Use Only information classifications, what are Company examples? *

(Insert company-specific examples)

As it relates to Public information classifications, what are Company examples? *

(Insert company-specific examples)

Integrity Protected classification indicates that the information, in electronic form, should be protected by Company-approved encryption or data inspection techniques that ensure the information has not been intentionally or inadvertently altered.

What are examples of this type of information? *

(Insert company-specific examples)

All Company information shall be classified in one of three availability categories:
• High • Medium • Low

A description of the High category information asset would be: *

(Insert company-specific examples)

Potential loss or impact to information within the High category would be: *

(Insert company-specific examples)

A description of the Medium category information asset would be: *

(Insert company-specific examples)

Potential loss or impact to information within the Medium category would be: *

(Insert company-specific examples)

A description of the Low category information asset would be: *

(Insert company-specific examples)

Potential loss or impact to information within the Low category would be: *

(Insert company-specific examples)

What email address shall we use to send you your policy group? *

Congratulations!
This concludes the policy creation questionnaire. Upon submission, you will find your policy suite downloadable under the My Documents tab. Thank you!

Submit

Powered by ITAM, the IT Audit Machine