CYBER ENTERPRISE SOLUTION

emergence

Operational Technology supplemental form

For the purpose of this supplemental form, Operational Technology (OT) means hardware and software used to monitor or control physical processes and industrial operations (including Industrial Controls Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Internet of Things (IOT)).

GENERAL

Policyholder name:

Please provide a brief overview of the OT used by the Policyholder including the total number of production/ manufacturing/distribution sites:

Sites operated by the Policyholder:

Sites operated by an Outsource Provider:

Does the Policyholder have an OT security policy that includes cybersecurity? ☐ Yes ☐ No

Does the Policyholder have a seperate OT cybersecurity budget? ☐ Yes ☐ No

GOVERNANCE

1. Who has responsibility for the cyber security of the Policyholder's OT?

ASSET MANAGEMENT

2. Does the policyholder maintain an asset inventory register of all OT assets including physical devices, software platforms and applications? ☐ Yes ☐ No

   Partial, please provide details:

ASSET SECURITY

3. Is the OT and IT environments segregated? ☐ Yes ☐ No

   If yes, please provide details of how it is segregated (e.g. air gaped, VLAN, DMZ etc):

4. Does segmentation exist between each of the sites to reduce the likelihood of multiple sites impacted by the same cyber event? ☐ Yes ☐ No

   If yes, please provide details of how they are segmented:

operational technology supplemental form

ASSET SECURITY (CONTINUED)

5. Does the Policyholder allow any remote access to their OT environment? ☐ Yes ☐ No

If yes, please outline how it is protected, managed, monitored and reviewed (e.g. multi-factor authentication, application allowlisting is employed to block unauthorised software from being installed run etc.):

6. Does the Policyholder allow remote access between the IT and OT environments? ☐ Yes ☐ No

If yes, please outline how it is protected, managed, monitored and reviewed:

7. Has the Policyholder implemented system hardening and application control in the OT environment? ☐ Yes ☐ No

If yes, please provide details (e.g. OT systems are blocked from accessing online services (e.g. web browsing, email etc.), application allowlisting is employed to block unauthorised software from being installed/run etc.)

8. Please describe the Policyholder's patch management process for the OT environment (including typical cadence, how the testing of patches is managed prior to rollout and any compensating controls until patches are completed):

9. Does the Policyholder carry out vulnerability scanning of the OT environment? ☐ Yes ☐ No

If yes, please outline the frequency:

☐ Annually ☐ Bi-annually ☐ Quarterly ☐ Monthly ☐ Other, please specify:

10. Does the Policyholder engage a third party to conduct regular information security audits and penetration testing of the OT environment? ☐ Yes ☐ No

If yes, please outline the frequency:

☐ Annually ☐ Bi-annually ☐ Quarterly ☐ Monthly ☐ Other, please specify:

operational technology supplemental form

ASSET SECURITY (CONTINUED)

11. Does the Policyholder utilise endpoint detection and response (EDR) software (or similar) within their OT environment? ☐ Yes ☐ No

- ☐ Yes, 100% covered
- ☐ Yes, less than 100% - please specify:
- ☐ No:

12. Are all alerts from the EDR software (or similar) fed into the SIEM (or similar) solution and monitored by the SOC 24/7?

☐ Yes ☐ No ☐ Partial, please provide further details:

13. How does the Policyholder manage privileged access to their OT environments? Please select all that apply:

- ☐ OT access rights are based on principle of least privilege
- ☐ Factory default settings (usernames/passwords) have been changed
- ☐ OT network administrators have separate accounts for 'regular' and privileged access
- ☐ Separate login credentials are used for access to IT and OT environments
- ☐ Local administrative rights are disabled on OT workstations
- ☐ Privileged access OT accounts are blocked from accessing online services (web browsing, email etc.)
- ☐ Multi-factor authentication is required for all privileged account access on workstations
- ☐ Credentials are managed, secured and rotated using a password vault
- ☐ Just-in-time access (which is time bound) methodology is utilised
- ☐ Other, please specify:

14. Does the Policyholder have any systems that do not have separate user and admin logons configured? If yes, please outline how are these systems protected, managed, monitored and reviewed:

15. Please outline the percentage (%) of OT that is considered "end of life" or "end of support" and what additional security measures have been implemented to prevent exploitation of any vulnerabilities. Please outline how business continuity will be ensured if this technology fails permanently:

operational technology supplemental form

RESILIENCY AND RECOVERY

16. Does the Policyholder maintain backups for the OT environment? ☐ Yes ☐ No
If yes, how are the backups secured:

- ☐ Offline / air gapped
- ☐ Encryption
- ☐ Vaulted credentials
- ☐ Access control listing
- ☐ Multi-factor authentication
- ☐ Immutable
- ☐ On a segmented and protected network
- ☐ Other, please specify:

17. Does the Policyholder conduct data and system restoration testing of the OT environment from backups ☐ Yes ☐ No

If yes, please outline how are these systems protected, managed, monitored and reviewed:

☐ Annually ☐ Bi-annually ☐ Quarterly ☐ Monthly ☐ Other, please specify:

18. Does the Policyholder have a Business Continuity Plan that specifically addresses recovery from a cybersecurity event within their OT environment, and has it been tested at least annually? ☐ Yes ☐ No

If no, can you please outline what business continuity measures are in place that are specific to the OT operations.

19. Does the Policyholder's Cyber Incident Response Plan (CIRP) specifically address their OT environment and tested at least annually? Please give details. ☐ Yes ☐ No

20. How much stockpiling of inventory does the Policyholder maintain as standard? Are any of those products only produced at a single site? Please give details.

operational technology supplemental form

RESILIENCY AND RECOVERY (CONTINUED)

21. At what capacity do each of the sites run at? In the event of one site being unavailable is there an ability for production to fail over to an alternative production site (or third-party production site) to maintain production throughput? Alternatively, are there any manual workarounds available?

22. Please outline if there are any single points of failure within critical applications in the IT/OT environment (e.g. any order/fulfilment applications that would impact the Policyholder's ability to provide products to customers) if so, please outline how these applications are hosted and secured and what redundancies are available (if any):

23. How does the Policyholder manage distribution? (e.g. in house or outsourced to a singular or multiple providers etc.)?

DECLARATION

I/we acknowledge that:

1. I/we have read and understood the important information provided on the last page of this document in the important information section.

2. I/we are authorised by all those seeking insurance to make this supplemental form, and declare all information on this supplemental form and any attachment is true and correct.

3. I/we authorise the underwriter to give to, or obtain from, other insurers or any credit reference service, any information relating to insurance held by me/us or any claim in relation thereto.

I/we acknowledge that, where answers are provided in the supplemental form are not in my/our handwriting, I/we have checked and certify that the answers are true and correct

Name:

Title:

Policyholder's signature:

Date: / /

It is important that you read and understand the following:

Claims made notice

Section C – Cyber & Privacy Liability and Section F – Optional Cover – Multimedia Liability Cover of this policy are issued on a 'claims made and notified' basis. This means that Section C – Cyber & Privacy Liability and Section F – Optional Cover Multimedia Liability Cover respond to:

a. Claims or multimedia claims first made against you during the policy period and notified to us during the policy period, provided you were not aware at any time prior to the commencement of the policy of circumstances which would have put a reasonable person in your position on notice that a claim or multimedia claim may be made against you; and

b. written notifications of facts pursuant to Section 40(3) of the Insurance Contracts Act 1984 (Cth). Effectively, the facts that you may decide to notify are those which might give rise to a claim or multimedia claim against you even if a claim or multimedia claim has not yet been made against you. If you decide to notify any such facts, such notification must be given as soon as reasonably practicable after you become aware of the facts and prior to the expiry of the policy period. If you give written notification of facts, the policy will respond to any claim or multimedia claim against you arising from those facts, even if the claim or multimedia claim is not made against you until after the policy has expired.

When the policy period expires, no new notification of facts can be made to us under the expired policy for a cyber event or multimedia injury first discovered or identified by you during the policy period.

Your duty of disclosure

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms. You have this duty until we agree to insure you. You have the same duty before you renew, replace, extend, vary, continue under similar insurance or reinstate an insurance policy. You do not need to tell us anything that:

– reduces the risk we insure you for; or
– is common knowledge; or
– we know or should know as an insurer; or
– we waive your duty to tell us about.

If you do not tell us anything you are required to, we may cancel your contract or reduce the amount we will pay you if you make a claim, or both.

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the policy as if it never existed.

About Emergence Insurance Pty Ltd

Before you enter into an insurance contract, you have a duty to Emergence Insurance Pty Ltd (ABN 46 133 037 153, AFSL 329634) ('Emergence') acts under a binding authority given to it by the insurer to administer and issue policies, alterations and renewals. In all aspects of arranging this policy, Emergence acts as an agent for the insurer and not for you.

Contact details are:
Email: info@emergenceinsurance.com.au
Telephone: 1300 799 562
Postal address: GPO Box R748, Royal Exchange, Sydney, NSW 2001

Privacy

In this Privacy Notice the use of "we", "our" or "us" means the Insurer and Emergence, unless specified otherwise.
We are committed to protecting your privacy.
We are bound by the obligations of the Privacy Act 1988 (Cth and the Australian Privacy Principles. These set out basic standards relating to the collection, use, storage and disclosure of personal information.
We need to collect, use and disclose your personal information (which may include sensitive information) in order to consider your application for insurance and to provide the cover you have chosen, administer the insurance and assess any claim. You can choose not to provide us with some of the details or all of your personal information, but this may affect our ability to provide the cover, administer the insurance or assess a claim.
The primary purpose for our collection and use of your personal information is to enable us to provide insurance services to you.
We may collect personal information in a number of ways, including directly from you via our website or by telephone or email.
Personal information will be obtained from individuals directly where possible and practicable to do so. Sometimes it may be collected indirectly (e.g. from your insurance intermediary or co-insureds). If you provide personal information for another person you represent to us that:
– you have the authority from them to do so and it is as if they provided it to us;
– you have made them aware that you will or may provide their personal information to us, the types of third parties we may provide it to, the relevant purposes we and the third parties we disclose it to will use it for, and how they can access it. If it is sensitive information we rely on you to have obtained their consent on these matters. If you have not done or will not do either of these things, you must tell us before you provide the relevant information.

We may disclose the personal information we collect to third parties who assist us in providing the above services, such as related entities, distributors, agents, insurers, reinsurers and service providers. Some of these third parties may be located outside of Australia, including New Zealand, Philippines, Vietnam, Malaysia and United Kingdom. In all instances where personal information may be disclosed to third parties who may be located overseas, we will take reasonable measures to ensure that the overseas recipieçnt holds and uses your personal information in accordance with the consent provided by you and in accordance with our obligations under The Privacy Act 1988 (Cth).
In dealing with us, you consent to us using and disclosing your personal information as set out in this statement. This consent remains valid unless you alter or revoke it by giving written notice to Emergence's Privacy Officer. However, should you choose to withdraw your consent, we may not be able to provide insurance services to you.
The Emergence Privacy Policy available at www.emergenceinsurance.com.au or by calling Emergence, sets out how:
– Emergence protects your personal information;
– you may access your personal information;
– you may correct your personal information held by us;
– you may complain about a breach of The Privacy Act 1988 (Cth) or Australian Privacy Principles and how Emergence will deal with such a complaint.
If you would like additional information about privacy or would like to obtain a copy of the Privacy Policy, please contact the Emergence Privacy Officer by:
Postal Address: GPO Box R748, Royal Exchange, Sydney NSW 2001
Phone: 1300 799 562
Email: privacyofficer@emergenceinsurance.com.au
You can download a copy of the Emergence Privacy Policy by visiting www.emergenceinsurance.com.au