PROPOSAL FORM
ANNUAL CYBER LIABILITY INSURANCE

NOTES

1. **Answer all questions fully, replies such as "see your records" or "previously advised" are not acceptable. If you have insufficient space to complete any of your answers, a separate sheet should be attached.**
2. **Signature of this Proposal does not bind the Proposer/ Insurers to complete the insurance.**
3. **In the case of a renewal, the Proposal needs to be completed and returned prior to renewal, to provide for continuation of cover.**

1. Company name and trading name:

_____ARMSCOR_____
_____

2. Physical Address:

370 Nossob Street, ErasumusKloof
_____
_____
0081
_____Code_____
_____
012428 1911 www.armscor.co.za
Telephone No: _____ Web Address
_____

Company Reg No: _____ VAT No: _____
info@armscor.co.za
E-mail address: _____

3. Names of any wholly owned subsidiaries: (if applicable)

_____
_____

_____
_____

4. If applicable, provide information on the level of integration and shared infrastructure with subsidiaries.

_____
_____

_____
_____

5. **Have you been involved in any mergers/acquisitions within the past 3 years?** YES/NO

6. **Do you have any planned mergers/acquisitions within the next 12 months?** YES/NO

7. Describe your business activities:

_____
_____

_____
_____

8. Products and Services offered:

_____
_____

_____
_____

9. Annual Turnover/Gross Revenue

Last Year _____Current Year
_____

10. Gross e-business revenue

Last Year _____Current Year
_____

11. Value of asset base

Last Year _____Current Year
_____

12. **Geographical split of gross revenue per region**:

South Africa: _____% Europe: _____ %

USA: _____% Other: _____ %

Africa (excl SA): _____ %

13. For countries outside South Africa, specify the countries:

_____
_____

14. Number of employees

Permanent: _____ Temporary: _____ Contractors: _____

15. Number of employees with system administration privileges.

Permanent: _____3_____ Temporary: _____0____ Contractors: ___0_____

16. Public facing URL addresses (websites and services such as file transfer facilities)

From internal network nothing. From DMZ www.armscor.co.za

_____

17. **Approximate number of external IP addresses on your network**

___25_____

18. **Approximate number of servers (including virtual machines) on your network**

__170_____

19. **Number of locations where servers are located**

_____6_

20. **Approximate number of laptops utilised**

____800____

21. **Approximate number of employees receiving company emails to privately owned devices**

__0_____

22. **Do you have a dedicated individual responsible for Information Security?** YES/NO

23. **Have you implemented information policies/procedures which have been approved by management?** YES/NO

24. **Have you communicated these policies/procedures to employees?** YES/NO

25. **Are security policies reviewed on an annual basis?** YES/NO The standard Armscor practice dictates 3 years but it is under review

26. Do you comply with privacy and data protection legislation applicable to all jurisdictions and

industry standards in which you operate? YES/NO

27. **Do you have a data classification policy including security requirements for sensitive data?** YES/NO

28. What security certification do you hold (for example PCI DSS/ISO27001)

_Quality to answer____

29. **Do you enforce a strong password policy across all accounts including:** YES/NO

Minimum password length restriction? ___8_____

Use of passwords which cannot within reason be deemed easily guessable? YES/NO

Do you perform testing for known trivial passwords (e.g. p@ssword1)? YES/NO

Account lockout as a result of how many failed authentication attempts? ____YES (5 attempts its under review)_____
Multi factor authentication? YES/NO

If no for any of the above, provide additional information on controls to manage authentication security

__Administrative controls_____

30. How regularly are users required to change their passwords?
Monthly (30 days)

---

31. After how many failed authentication attempts are accounts locked out?
5 attempts

---

32. How long are accounts locked out for after failed authentication attempts?
Until account is reset

---

33. **Are users prevented from re-using their passwords for at least 5 changes?** YES/NO
If not, how many changes? _____

34. Are password rules enforced on all sensitive systems, e.g., password parameters defined on active directory? YES/NO

35. **How frequently are your IT environments subjected to vulnerability scans or penetration testing?**
Quarterly

_____

Please attach the latest testing report

Were serious concerns raised at your last test and have these been addressed? YES/NO
If all serious concerns have not been implemented, provide details of outstanding items with remediation actions to be taken and associated timelines:

Attached table in Appendix A

_____

_____

_____

_____

_____

_____

36. **Did the scope of the testing performed include both your internal and external IT environment?** YES/NO

37. **Do you perform penetration testing and/or secure code reviews on all new systems/software prior to deployment?** YES/NO

38. **How frequently are your IT environments subjected to penetration testing?** _____N/A _(Closed network)_____ *Please attached the latest report*

Were any serious concerns raised at your last test and have these been addressed? YES/NO

39. **How frequently are your IT environments subjected to third party security assessments, including vulnerability scanning?** *Please attach the latest testing report*
N/A

_____

_____

Where any serious concerns raised at your last test and have these been addressed? YES/NO

If all serious concerns have not been implemented, please provide details of outstanding items with remediation actions to be taken and associated timelines:

_____

_____

_____
_____

40. For sensitive servers and devices do you actively maintain:

System Activity Logs YES/NO and for what period of Time _6 months_____

Security Logs YES/NO and for what period of Time _____6 months_____

41. How regularly do you review the logs?
_____**Monthly**_____

42. **Do you investigate all violations, intrusions and irregularities noted in the logs?** YES/NO

43. To determine your potential data exposure, provide the approximate number of employee and client unique data records that you have collected/stored/processed for each of the following data types:

Bank records or financial account details: **YES/NO** **Number of records:**
_____

(this will include staff bank details/client bank or financial records)

Medical records or health information: **YES/NO** **Number of records:**
_____

(includes medical information of clients or employees eg: medical procedures or diagnosis information)

Payment card details: **YES/NO** **Number of records**
_____

Do you store the card number? YES/NO
Do you store the card expiry date? YES/NO
Do you store the card validation codes (CVV number)? YES/NO
Do you have card terminals YES/NO
(if yes, do you store the card details) YES/NO
(or do you have a third party who owns, controls, manages the device?) YES/NO

Personal identity information **YES/NO** **Number of records**
_____

(names, ID numbers, contact details, address of employees, clients, contractors, suppliers, etc)

Third party corporate confidential data **YES/NO** **Number of records**
_____

(not common knowledge or publicly available information. Eg: trade secrets, annual financial statements,

SLA's, designs, etc)

44. **Do you make use of or provide any web application functionality?** YES/NO
Please provide details ____Mimecast, tender system_____

45. **Have you configured your network and externally visible applications and services to ensure that access to sensitive data is restricted to properly authorised requests**? YES/NO

46. Have you implemented data retention and secure destruction policies for physical and electronic data and assets? YES/NO

47. **Have you disable employee write access to USB devices?** YES/NO

48. **Have your internet facing systems been configured so that no sensitive or personal data resides directly on them, but is instead stored behind a firewall on internal databases/systems** YES/NO

49. Have you implemented encryption for the following?

- Data stored on portable devices (laptops, external storage devices, tablets, phones, etc.) YES/NO
- Sensitive data transmitted outside your environment YES/NO
- Sensitive data/backups stored outside your environment YES/NO N/A
- Sensitive data stored in your environment YES/NO *If YES, please provide additional information*

BitLocker for endpoints and classified storage

_____
_____

_____
_____

50. **Do you operate a local network or operate solely on cloud services?** _Local network___

51. Please indicate which of the following you have implemented (select all that apply)

- Endpoint protection (eg Anti-virus) which is updated per vendor recommendations? YES/NO

If Yes, specify the endpoint protection you have implemented: _____**Ivanti and AVG**_____

- Next generation firewalls at all breakout points to external networks? YES/NO

If Yes, please specify the firewall technology you have implemented: ____**Checkpoint ,CISCO and PFSENSE**_____

- Segmentation to protect sensitive data and resources within the network? YES/NO

- Web application firewalls (WAF) YES/NO

- Proactive monitoring of access to sensitive/critical servers, data and applications? YES/NO

If Yes, provide additional information on the monitoring performed including technologies used:
AD Audit and TACACS
_____
_____

- Cyber threat intelligence (CTI) function YES/NO

- Data loss prevention (DLP) tools YES/NO

- Mobile Device Management (MDM) incl access control and remote device wipe YES/NO

- Email security including URL rewriting, malware protection and protection against Impersonation YES/NO

If Yes, specify the email technology implemented:
_____**Mailmarshal**_____

52. **Have you implemented anti-virus software on all computers and mission critical servers?** YES/NO

53. **As part of system configuration do you ensure that all default vendor accounts are secured, via disabling/deleting or changing the account password?** YES/NO

54. **Do you secure all computers and servers according to your technical security configuration standards?**

YES/NO
If Yes, provide additional information on the sources consulted to define technical security configuration standards:_____Microsoft best practices and Armscor policies and practices_____
_____

55. **Do you manage access permissions, incl application of the principles of least privilege and separation of duties?** YES/NO

56. **Have you implemented controls to restrict unauthorised access to sensitive data via your wireless network?** YES/NO

57. **Have you implemented physical controls such as surveillance cameras or access control mechanisms to restrict access to your server room and other sensitive processing facilities** YES/NO

58. **Have you implemented a formal control process including risk assessments, testing, approval and roll back?** YES/NO

59. **How long after release do you implement security related patches and updates on computers, servers and network appliances (routers, firewalls, etc.)?** Monthly, unless it's critical it is attended immediately

60. **Are you making use of any unsupported software or operating systems?** YES/NO
If Yes, please provide additional information including: whether these are visible to external networks, the nature of data and/or systems running on these, any controls implemented to mitigate the risk and plans to remediate.

____Not visible to external network and in process of replacing with ERP system_____
_____

_____
_____

61. **Do you allow for remote access to your network?** YES/NO

If Yes, is remote access exclusively over secured channels (eg: VPN) with multifactor authentication? YES/NO VPN without MFA

If Yes, are control implemented to protect accounts including installation and administration accounts from brute force password attacks? YES/NO

If Yes, please provide addition information on the controls implemented to secure remote access including controls to protect against brute force password attacks:

_____
_____

_____
_____

62. **Do you store or process payment card data?** YES/NO

If Yes,What level PCI merchant have you been certified as?
_____

What is your estimated number of payment card transactions processed per year? _____

Are you fully compliant with the EMV card processing standards?
YES/NO

Does a third-party process payment card data on behalf?
YES/NO
If Yes, Provide the name of the payment processor _____

Do you have evidence that the payment processor is PCI certified?
YES/NO

Is payment card data encrypted or tokenised at all times?
YES/NO

Are your point of sale (POS) terminals designed to be tamper proof?
YES/NO

Do you segregate your payment network from your normal network?
YES/NO

Are POS terminals standalone or integrated with your systems? _____

How frequently are your POS devices scanned for malware or skimming devices? _____

How frequently is your payment network subjected to third party testing? _____

Where any serious concerns raised at your last test and have these been addressed?

_____
_____

67. THIRD PARTY SERVICE PROVIDERS

Functions	Outsourced to third party provider	Third party providers name
Cloud data processing/storage	YES/NO	
Data centre/hosting	YES/NO	
Data processing (marketing/payroll)	YES/NO	
Managed security services	YES/NO	
Network implementation/maintenance	YES/NO	
Off-site archiving, backup and/or storage	YES/NO	
Payment processing	YES/NO	ABSA

Software implementation/maintenance	YES/NO	Nessus and Mailmarshal
Systems development, customisation and maintenance	YES/NO	
Other (please specify)	YES/NO	

68. What level of access do you grant to third party service providers?
Local admin access not Super user Admin access/ Full access

---

69. Do agreements with third party service providers require levels of security commensurate with your information security policies? YES/NO

70. Do you review that third party service providers are adhering to contractual and/or regulatory requirements regarding data protection? YES/NO

71. Do you require indemnification from third party service providers for any liability attributable to them (including data breach and system downtime) YES/NO

72. Indicate the time after which a disruption or failure of your IT environment, including network and applications, would have a significant impact on your revenue and operations?
BCP_____

73. Do you have an incident response plan including a team with defined roles and responsibilities? YES/NO

If Yes, how frequently do you review, test and/or update the plan? Yearly _____

74. Do you keep an incident log of all data security breaches and network failures? YES/NO

75. Are incidents investigated and escalated based on severity? YES/NO

76. Do you have documented and approved disaster recovery and business continuity plans? YES/NO

If Yes, How long will it take you to be operational following an incident? ___Refer to BCP (check BCP)_____

What is your anticipated potential data loss? 24 hrs maximum

How frequently do you review, test and update such plans? Bi-annually

77. Are copies of your incident response, business continuity and/or disaster recovery plans kept in hard copy or in a separate and secure environment so that they are accessible in the event of a full network outage? YES/NO

78. Do you have third party service providers who you are dependent upon to have incident response,
business continuity and/or disaster recovery plans? YES/NO

If Yes, do you review the adequacy of the plans? YES/NO

79. How frequently do you generate backups? Daily

If backups are generated, do you at any time always have a backup copy which is not connected to or accessible via your network? YES/NO

80. Do you monitor for the successful generation of backups? YES/NO

81. How frequently do you perform restoration testing of backups? Monthly

82. Please provide information on the impact a disruption or failure of your IT environment would have on your operations (please include estimates on impact to revenue and third parties)

_____Check BCP_____

83. Please provide information on measures implemented to prevent and/or mitigate the impact of a disruption or failure of you IT environment including network and applications:

- **Firewalls security**
- **Endpoint protection**
- **Email protection**

---

84. Do you conduct background checks on potential employees as part of the recruitment process?

YES/NO

85. Do you have a process implemented for granting, reviewing and disabling user accounts and privileges? YES/NO

86. How long after termination of employment do you typically revoke user privileges?
Last day of service

---

87. Have employees been required to attend any security/data privacy training/awareness courses within the past 12 months? YES/NO

88. Have you implemented controls to manage and/or restrict internet access and usage? YES/NO

89. Do you restrict user access based on job function and review access on an annual basis? YES/NO

90. Does employee awareness training include targeted phishing campaigns and/or assessments to test
Understanding? YES/NO

91. Do you have a formal review process for both online and offline content prior to publishing? YES/NO
If Yes, are such review performed by a qualified legal resource? YES/NO

92. Do you make use of any copyrighted material provided by others? YES/NO
If Yes, do you obtain written permission to use such material and confirm that use thereof does not infringe upon any intellectual property rights? YES/NO

93. Do you provide any platforms or forums which users can post or upload their own content to?

Y
ES/
NO

If Yes, Is such content reviewed before publishing? YES/NO

Do you have a process for quickly removing any offending content? YES/NO

94. Biometric data:

Have you at any time in the last 5 years or are you currently collecting any biometric data on employees or consumers as defined by law including (but not limited to):

Retina scan
YES/NO

Iris scan
YES/NO
Fingerprint
YES/NO
Voiceprint
YES/NO
Hand scan
YES/NO
Face geometry
YES/NO

Have you on all occasions obtained written consent from employees/consumers/individuals prior to collection
of their biometric data? YES/NO

Do you clearly define to employees/consumers/individuals how you will collect their biometric data, how it will
be stored and when it will be destroyed? YES/NO

Do you sell, lease, trade or otherwise profit from an employee's/consumers/individual's biometric data? YES/NO

How do you store the biometric data?
All data is stored in the dedicated computer for the Security Access Control System only

What level of security do you have applied to biometric data for storage and transmission?
Confidential

Is it stored separately/segmented from other types of data?
It's not stored separately, the database form has all the fields to be used for different types of access control, these fields are either enabled or disabled depending on the type of access authorised.

Do you define who will have access to this data?
Only Authorised Security Officers trained to enrol employees on the database have access, the database is password protected

Do you have a biometric data retention schedule outlining how long you will hold the biometric data for?

No, we deactivate the access control authorisations and information is kept on the database.

Do you have a data destruction policy for biometric data the business no longer needs as soon as practicable and in line with legal requirements and as soon as practical?

An Armscor Security Instruction (A-WI-014) for the disposal of hardware containing this biometric data is being used, the computer housing the database is not on any network, it is stored in a security room where access is restricted to Security Officers and the need to dispose of this computer has not arisen

Have you received any complaints alleging the unlawful collection, use, dissemination, or sale of biometric data?

No complaints were registered for misuse or dissemination of biometric data

Claims and Insurance History

If YES, please provide FULL information

95. **Have you ever had an insurance policy cancelled or been declined insurance cover?**

_____

96. **Are you or any of the partners, directors or officers, aware of or are there any circumstances within the past 5 years that would have given, may give, or have given, rise to a claim against the organisation or against this insurance policy?**

_____

97. **Have you suffered from any of the following within the past 5 years:**

- Systems intrusion, tempering, malicious code attack, loss of data, extortion attempt, data theft or similar? YES/NO
- Unauthorised transmission or disclosure of sensitive information for which you are responsible? YES/NO
- Allegations of invasion of privacy, that sensitive information has been compromised or content infringement? YES/NO
- An unscheduled network outage or interruption? YES/NO