CYBER INSURANCE PROPOSAL FORM

Please answer **ALL** questions completely.
Should any question or part thereof not be applicable, please state "N/A".
Should insufficient space be provided, please continue on your company letterhead.

1. Name of Insured: National Home Builders Registration Council (NHBRC)
2. Physical address: 27 Leeuwkop Road, Sunninghill, Johannesburg — Post code: 2157
3. Primary contact phone number: (011) 317-0459
4. Primary contact email address: nthethih@nhbrc.org.za
5. Registration number: n/a — 6. VAT number: n/a
7. Choose an item which closely matches primary nature of business: Government Agency
   If Other, please specify:
8. Products and services offered
   The Regulator Of The Home Building Industry
9. Subsidiary names (if applicable)
   n/a
10. If applicable, please provide additional information on the level of integration and shared infrastructure with subsidiaries
11. Have you been involved in any mergers/acquisitions within the past 3 years? No mergers or acquisitions
12. Do you have any planned mergers/acquisitions within the next 12 months? Yes ☐ No ☑
13. Revenue

Annual revenue	Last year	R 2,426,832,924.00	Current year	R 1,702,768,799.00
Gross e-business revenue	Last year	R	Current year	R

14. Geographical split of gross revenue by region

South Africa	Last year	100.00 %	Current year	100.00 %
Africa (excl. SA)	Last year	%	Current year	%
Europe	Last year	%	Current year	%
USA	Last year	%	Current year	%
Other	Last year	%	Current year	%

For countries outside South Africa, please specify the countries

15. Number of employees

Permanent	535	Contractors		Temporary	35

16. Number of employees with system administration privileges

Permanent	3	Contractors		Temporary	0

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

www.nhbrc.org.za

18. Approximate number of external IP addresses on your network: 11 - 25

19. Approximate number of servers (including virtual machines) on your network: 11 - 25

20. Number of locations where servers are located: 2

21. Approximate number of laptops utilised: 501 - 1 000

22. Approximate number of employees receiving company emails to privately owned devices: 501 - 1 000

Security Policies and Standards

1. Do you have a dedicated individual responsible for Information Security?

Yes CISO, CIO or equivalent

2. Have you implemented information security policies/procedures and communicated these to employees? Yes ✓ No

3. Are your security policies reviewed on at least an annual basis? Yes ✓ No

4. Do you comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which you operate? Yes ✓ No

5. Do you have a data classification policy including security requirements for sensitive data? Yes ✓ No

6. Please specify any security certifications you hold (for example PCI DSS)

We comply, but we do not have a certificate

7. Do you enforce a "strong password policy" across all accounts, including:

- Minimum password length restriction: 8 - 10 characters
- Use of passwords which cannot within reason be deemed easily guessable: Yes ✓ No
  - Do you perform any testing for known trivial passwords such as p@ssword1: Yes ✓ No
- Account lockout as a result of failed authentication attempts: After 5 failed attempts
- Multi factor authentication: Yes ✓ No

If No to any of the above, please provide additional information on controls to manage authentication security

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

- System activity logs: Yes ✓ No — and for what period of time: Less than 1 year
- Security logs: Yes ✓ No — and for what period of time: Less than 1 year

9. How regularly do you review the logs? Weekly

10. Do you investigate all violations, intrusions and irregularities noted in the logs? Yes ✓ No

BH

Security Reviews and Assessments

1. How frequently are your IT environments subjected to penetration testing? Annually

   Please attach the latest testing report

   - Were any serious concerns raised at your last test and have these been addressed? Still to address serious concerns

2. How frequently are your IT environments subjected to third party security assessments, including vulnerability scanning? Annually

   Please attach the latest testing report

   - Were any serious concerns raised at your last test and have these been addressed? Still to address serious concerns

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

   External Network -Prevent the public from reading .htaccess files -WordPress fixes etc.

3. Did the scope of the testing performed include both your internal and external IT environment? Yes ☑ No ☐

4. Do you perform penetration testing and/or secure code reviews on all new systems/software prior to deployment? Yes ☑ No ☐

Sensitive and Private Information

1. To determine your potential data exposure, please 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	Less than 500 000
Medical records or health information	Less than 1 000
Payment card details	Less than 25 000
• 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 ☑
Personal identity information (names, ID numbers, contact details, addresses)	Less than 1 000 000
Third party corporate confidential data	Less than 500 000

2. Do you make use of or provide any web application functionality? Multiple of the above

3. 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 ☐

4. Have you implemented data retention and secure destruction policies for physical and electronic data and assets? Yes ☑ No ☐

5. Have you disabled employee write access to USB devices? Yes ☐ No ☑

6. 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 ☐
   - Sensitive data stored in your environment (data at rest) Yes ☑ No ☐

   If Yes, please provide additional information

   Encryption Method: BitLocker

BH

Payment Card Data

Please complete this section only if you store or process payment card data

1. What level PCI merchant have you been certified as? Not applicable
2. What is your estimated number of payment card transactions processed per year? 5 000 000
3. Are you fully compliant with the EMV card processing standards? Yes ✓ No
4. Does a third party process payment card data on your behalf? Yes ✓ No

   If Yes, please provide the name of the payment processor FNB

   If Yes, has the payment processor provided you with evidence that they are PCI certified? Yes ✓ No
5. Is payment card data encrypted or tokenised at all times? I don't know Yes ✓ No
6. Are your point of sale (POS) terminals designed to be tamper proof? Yes ✓ No
7. Do you segregate your payment network from your normal network? N/A Yes No
8. Are POS terminals standalone or integrated with your systems? Standalone with no integration
9. How frequently are your POS devices scanned for malware or skimming devices? Every 6 months
10. How frequently is your payment network subjected to third party testing? Every 6 months
    - Were any serious concerns raised at your last test and have these been addressed?

    No concerns were raised

Security Implementation

1. Do you operate a local network or operate solely on cloud services? Local network and cloud services
2. Please indicate which of the following you have implemented (please select all that apply):
   - Endpoint protection (e.g. Anti-virus) which is updated per vendor recommendations Yes ✓

     If Yes, please specify the endpoint protection you have implemented Microsoft defender
   - Next generation firewalls at all breakout points to external networks Yes ✓

     If Yes, please specify the firewall technology you have implemented Fortinet
   - Segmentation to protect sensitive data and resources within the network? Yes ✓
   - Web application firewalls (WAF) Yes ✓
   - Proactive monitoring of access to sensitive/critical servers, data and applications Yes ✓

     If Yes, please provide additional information on the monitoring performed including technologies being used

     Microsoft Sentinel
   - Cyber threat intelligence (CTI) function Yes ✓
   - Data loss prevention (DLP) tools Yes ✓
   - Mobile Device Management (MDM) including access control and remote device wipe Yes ✓
   - Email security including URL rewriting, malware protection and protection against impersonation attacks Yes ✓

     If Yes, please specify the email security technology implemented Microsoft Defender for Office 365
3. As part of system configuration do you ensure that all default installation and vendor accounts are secured via changing the account password and where possible disabling, deleting or renaming the account? N/A Yes ✓ No

4. Do you manage access permissions, including application of the principles of least privilege and separation of duties?

Yes for installation, service and user accounts

5. Do you secure all computers, servers and applications according to your technical security configuration standards? Yes ✓ No

If Yes, please provide additional information on the sources consulted to define technical security configuration standards

CIS, PCI , ISO 270001

6. Have you implemented a formal change control process including risk assessments, testing, approval and roll back? N/A Yes ✓ No

7. Have you implemented controls to restrict unauthorised access to sensitive data via your wireless network? N/A Yes ✓ No

8. Do you allow for remote access to your network? Yes, to employees and third parties

If Yes, is remote access exclusively over secured channels (for example Virtual Private Network (VPN) with multi factor authentication)? Yes ✓ No

If Yes, are controls implemented to protect accounts including installation and administration accounts from brute force password attacks? Yes ✓ No

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

Multi-Factor Authentication (MFA), Microsoft Privileged Identity Management, VPN

Account Lockout Policies, Password Policies

9. How long after release do you implement security related patches and updates on computers, servers and network appliances (routers, firewalls, etc.)? Monthly

10. Have you implemented physical controls such as reception or access control mechanisms to restrict access to your offices, server room and other sensitive processing facilities? Yes ✓ No

11. 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

Windows 2012 -SAP upgrade underway

Third Party Service Providers

Function	Outsourced		Third party provider's name
Cloud data processing/storage	Yes ✓	No	BCX, Microsoft
Data centre/hosting	Yes ✓	No	BCX and Microsoft
Data processing (marketing/payroll)	Yes	No ✓	
Managed security services	Yes	No ✓	
Network implementation/maintenance	Yes ✓	No	BCX
Off-site archiving, backup and/or storage	Yes ✓	No	BCX
Payment processing	Yes ✓	No	Hyphen
Software implementation/maintenance	Yes	No ✓	
Systems development, customisation and maintenance	Yes ✓	No	Purple Wire, VTTV
Other (please specify)	Yes	No	

BH

1. What level of access do you grant to third party service providers? Restricted access

2. Do agreements with third party service providers require levels of security commensurate with your information security policies? N/A ☐ Yes ☑ No ☐

3. Do you review that third party service providers are adhering to contractual and/or regulatory requirements regarding data protection? N/A ☐ Yes ☑ No ☐

4. Do you require indemnification from third party service providers for any liability attributable to them (including data breach and system downtime)? N/A ☐ Yes ☑ No ☐

Incident Response, Business Continuity and Disaster Recovery Planning

1. Please 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: After 48 hours

2. 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 incident response plan? Annually

3. Do you keep an incident log of all data security breaches and network failures? Yes ☑ No ☐

   If Yes, are incidents investigated and escalated based on severity? Yes ☑ No ☐

4. Do you have documented and approved disaster recovery and business continuity plans? Yes ☑ No ☐

   If Yes, how long would it take you to be operational following an incident? Within 1 week

   If Yes, what is your anticipated potential data loss? Up to 24 hours of data

   If Yes, how frequently do you review, test and update such plans? Annually

5. 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 ☐

6. Do you have any 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 such plans? Yes ☑ No ☐

7. 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?

   Offsite at a secure location connected to the main network

8. Do you monitor for the successful generation of backups? Yes ☑ No ☐

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

10. 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)

    BCM

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

    Disaster recoverty plan , tested and implemented.

    Proactively monitor our environment to identify issues that could lead to system downtime

Personnel Security

1. Do you conduct background checks on potential employees as part of the recruitment process? Yes ✓ No
2. Do you restrict user access based on job function and review access on at least an annual basis? Yes ✓ No
3. How long after termination of employment do you typically revoke user access privileges? A day
4. Have you conducted any security/data/privacy training/awareness courses for employees within the past 12 months? Yes ✓ No
5. Does employee awareness training include targeted phishing campaigns and/or assessments to test understanding? Yes ✓ No

Digital Media Liability

1. Do you have a formal review process for both online and offline content prior to publishing? Yes ✓ No

   If Yes, are such reviews performed by a qualified legal resource? Yes ✓ No
2. 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
3. Do you provide any platforms or forums which users can post or upload their own content to? Yes No ✓

   If Yes, is such content reviewed before publishing? Yes No ✓

   If Yes, do you have a process for quickly removing any offending content? Yes No ✓

Claims and Insurance History

1. Have you ever had an insurance policy cancelled or been declined insurance cover? Yes No ✓
2. Have you suffered from any of the following within the past 5 years:
   - Systems intrusion, tampering, 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
3. 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? Yes No ✓

   If Yes, to any of the above, please provide additional information including nature of the incident, damages incurred and remediation action taken

Limit of Indemnity

	Option 1	Option 2	Option 3	Option 4
Quote	R 20,000,000.00	R 25,000,000.00	R 30,000,000.00	R 40,000,000.00
Deductible	R 500,000.00	R 500,000.00	R 500,000.00	R 500,000.00

R-H

Privacy Clause

In order to provide you with insurance, we have to process your personal information. We will share your personal information with other insurers, industry bodies, credit agencies and service providers. This includes information about your insurance, claims and premium payments. We do this to provide insurance services, prevent fraud, assess claims and conduct surveys. We will treat your personal information with caution and have put reasonable security measures in place to protect it. By signing this application for insurance, you agree to the processing and sharing of your personal information.

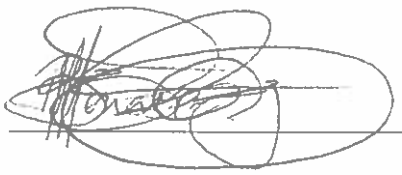
Declaration

I/We, the undersigned, declare that the statements set forth in this proposal form together with any other information supplied are true and correct and that I/we have not misstated or suppressed any material facts.

I/We agree that this proposal form together with any other information supplied by me/us shall form the basis upon which the contract of insurance is concluded and shall be incorporated therein.

I/We further undertake that in the event that the information provided changes between the date of this application and inception of cover, I/We will notify iTOO of such changes as soon as reasonably possible.

Bongani Monareng - Acting Chief Risk Officer	Acting Chief Risk Officer
Name (duly authorised)	Designation

Signature 

Date

2	0	2	6	0	2	0	6