Responsible Disclosure Statement

We at IndusInd Bank has great concern for the security of its banking systems including online digital platform and are committed about our customer's data's confidentiality, integrity, availability and privacy. We blend security at multiple steps within our products with state of the art technology to ensure our systems maintain strong security measures.

If you are a security researcher and have discovered a security vulnerability in one of our services, we appreciate your help in disclosing it to us in a responsible manner. We will validate and fix vulnerabilities in accordance with our policies. IndusInd Bank reserves all of its legal rights in the event of any noncompliance to the applicable laws and regulations.

Rules for Finding and Reporting Security Vulnerabilities

- Take responsibility and act with extreme care and caution
- When investigating the matter, only use methods or techniques that are compliant with law
- Take necessary actions ONLY to find or demonstrate the weaknesses
- DO NOT exploit any weakness/vulnerability
- Always be compliant with this Statement
- Do not put any customer or IndusInd Bank data at risk, degrade any of our system's performance
- If your actions are intrusive or an attack on our system, we may take action against the same including reporting them to law enforcement agencies
- IndusInd Bank reserves its right to initiate legal action against any person and/or report to relevant authorities of such person who conduct any Tests or investigations which are prohibitive or not in compliance with law or not as per this Statement
- Do not posting, transmitting, uploading, linking to, sending, or storing any malicious software
- Do not testing third-party applications, websites, or services that integrate with or link to IndusInd Bank's network

Reporting:

The safety of our customers' information and assets is our top priority. Therefore, we encourage anyone, who have discovered a vulnerability in our systems to act instantly and help us improve and strengthen the safety.

DO NOT PUBLICLY ANNOUNCE THE VULNERABILITY OVER PUBLIC FORUMS OR ANY SOCIAL MEDIA CHANNELS, BUT GET IN TOUCH WITH US IMMEDIATELY AND GIVE US THE TIME TO EXAMINE THE ISSUE.

If you believe you’ve found a security issue in one of our products or services, please send it to us on **incidentresponse@indusind.com** along with your contact details and include the following in your report:

- A description of the issue identified
- Where the issue is located (e.g. module, web page, application etc.) along with screenshots
- Description of the steps required to reproduce the issue

A few examples of vulnerabilities include:

- Authentication flaws and Improper access control
- Circumventing of platform and/or privacy permissions
- Privilege escalations
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Server-Side request forgery (XSRF)
- Injection Attacks (SQL, XML, JSON, OS Command Injection, LDAP and XPath injection etc.)
- Business logic Bypass
- Arbitrary redirect (directory traversal, failure to restrict user access to functions etc.)
- Insecure communications
- Improper error handling
- Insecure direct object references
- Server-side code execution (RCE)
- Broken authentication and session management

Prohibited actions:

- Do not use vulnerability you discover for purposes other than your own investigation
- Do not use social engineering to gain access to a system
- Do not install any back doors – not even to demonstrate the vulnerability of a system
- Do not alter or delete any information/configuration in the system
- Do not share access or details of any vulnerable system with others
- Do not use brute force techniques, such as repeatedly entering passwords, to gain access to systems
- Do not access, Download, or Modify data residing in an account that does not belong to you or attempt to do any of the foregoing
- If you need to copy information for your investigation:
    - Never copy any of the customer information
    - If one record is sufficient, do not go any further
    - Always ensure that data you are copying has sensitive information redacted
- Do not perform any executing or attempting to execute any “Denial of Service” attack
- Do not post, transmit, upload, link, send, or store any malicious software or code

- Do not perform testing in a manner that would result in the sending unsolicited or unauthorized junk mail, spam, pyramid schemes, or other forms of duplicative or unsolicited messages
- Do not perform testing in a manner that would degrade the operation of any IndusInd Bank properties; or testing third-party applications, websites, or services that integrate with or link to IndusInd Bank properties.
- Do not perform testing with out-dated or unpatched browsers and operating systems
- Do not disable Secure flag on non-sensitive cookies
- Do not enable HTTP Only flag on non-sensitive cookies
- Do not exploit security vulnerabilities in third-party websites and applications that integrate with issues

NON-COMPLIANCE

Public disclosure of any submission details of an identified or alleged vulnerability without written consent from IBL will make cause the submission to be non-compliant with this Responsible Disclosure Statement. In addition, to remain compliant you are prohibited from:

- posting, transmitting, uploading, linking to, sending, or storing any malicious software
- testing third-party applications, websites, or services that integrate with or link to IndusInd Bank properties

Our Recognition

If you identify a valid security vulnerability in compliance with this Responsible Disclosure Statement, IndusInd Bank shall –

- Acknowledge receipt of your vulnerability report
- Work with you to understand and validate the issue
- Address the risk as deemed appropriate by IndusInd Bank team
- Work together to prevent cyber-crime.

IndusInd Bank will review the submission to determine if the finding is valid and has not been previously reported. Publicly disclosing the submission details of any identified or alleged vulnerability without express written consent from IndusInd Bank will deem the submission as noncompliant with this Responsible Disclosure Statement.