IDFC, as a provider of financial services, takes security issues very seriously and recognize the importance of privacy, security, and community outreach. As such, we are committed to addressing and reporting security issues through a coordinated and constructive approach designed to drive the greatest protection for our customers. Whether you're our customer, a user of our services, a software developer, or simply a security enthusiast, you're an important part of this process.

Have you discovered a security flaw in a system belonging to IDFC? Please notify us before informing the outside world, so that we can first take action. Doing so is called 'responsible disclosure'.
Do you have the skills and have you discovered any vulnerabilities in our systems? Please help by reporting these vulnerabilities to us, so that we can improve the safety and reliability of our systems together. A team of security experts will investigate your finding/findings. You will receive an e-mail with an initial reply within two working days. However, there may be a delay in responding due to workload or holidays.

Please note: going public with your finding before we have fixed it will exclude you from the "reward". Instead, please talk to our experts and give them time to assess and solve the problem.
The scope of this will be IDFC Bank website, Retail & Mobile internet banking websites, and/or systems.

1. www.idfcbank.com
2. secured.idfcbank.com
3. my.idfcbank.com

You may NOT use this programme for the following:

- Reporting complaints about IDFC's services or products
- Questions and complaints about the availability of IDFC websites, mobile banking, or internet banking
- Reporting monetary issues (e.g. ATM's and PIN devices)
- Reporting Fraud or the presumption of fraud
- Reporting fake e-mails or phishing e-mails (report these to report.phishing@idfcbank.com)
- Reporting malware

Please respect the following programme rules before reporting a vulnerability:

Take responsibility and act with extreme care and caution. When investigating the matter, only use methods or techniques that are necessary to find or demonstrate the weaknesses. It's important to ensure that you Secure your own systems as tightly as possible.

- Make sure that during your and our investigation of your reported vulnerability, you do not cause any damage to our systems
- Do not utilize social engineering to gain access to our IT systems
- Never let your investigation disrupt our online and other services
- Never publicize any bank or customer data that you may have found during your investigation
- Do not put a backdoor in the system, not even for the purpose of showing the vulnerability. Inserting a backdoor will cause even more damage to the safety of our systems
- Do not make any changes to or delete data from the system. If your finding requires you to copy the data from the system, do not copy more data than necessary. If one record is sufficient, do not copy any more
- Do not make any changes to the system
- Do not attempt to penetrate the system any further than required for the purpose of your investigation. Should you have successfully penetrated the system, do not share this gained access with any others
- Do not utilize any brute-force techniques (e.g. repeatedly entering passwords) in order to gain access to the system
- Do not use techniques that can affect the availability of our online and other services
- If your reported vulnerabilities have been solved or have resulted in a change in our services, you will be eligible for a reward
- Vulnerabilities detected by IDFC employees/former employees of IDFC & already empaneled Third party service providers are excluded from any rewards
- If your reported vulnerability has also been reported by others, the reward will be granted to the individual who first reported it
- Multiple reports for the same vulnerability type with minor differences will be treated as one report (only one submission will be rewarded)
- If you are eligible for a reward, we will require your personal information to provide you with the reward.

Law and regulations: Your investigation of our IT systems could be regarded as criminal under local or international law and you may then risk criminal prosecution. If you have detected vulnerabilities in one of our IDFC pages, please be aware that local law takes precedence over IDFC rules. Nevertheless, if you act in good faith and according to IDFC's rules, we will not report your actions to the authorities, unless required to do so by law.

Your privacy: We will only use your personal information to get in contact with you and to undertake actions with regard to your reported vulnerability. We will not distribute your personal information to third parties without your permission, unless we are required to do so by law, or if an external organization takes over the investigation of your reported vulnerability. In that case, we will make sure that the relevant authority treats your personal information confidentially.

Reporting a vulnerability: You can report a vulnerability by sending an e-mail to: **responsible.disclosure@idfcbank.com**. A prerequisite for sending an e-mail to the above-mentioned e-mail address is that you use the public PGP key (zip). Please write your report in a clear and concise way, including the following in particular:

- Software/Product(s) containing the vulnerability (this could include websites / mobile applications / MATM etc):
- Vulnerability Description:
- How may an attacker exploit this vulnerability? (Proof of Concept):
- What is the impact of exploiting this vulnerability?
- How and when did you find the vulnerability? (Be specific about tools and versions you used.)

Disclosure Plans

- Have you already reported this vulnerability to any vendors or any other organizations:?
- Is this vulnerability being publicly discussed? YES/NO, if yes then provide URL.
- Is there evidence that this vulnerability is being actively exploited? YES/NO, if yes, then provide URL/evidence.
- Do you plan to publicly disclose this vulnerability
    - on this date: (Please include your time zone.)
    - at this URL:

Reporter

- Name:
- Organization:
- Email:
- Telephone:
- May we provide your contact information to third parties? YES/NO

Important note: Submissions may stand closed if reporter is non-responsive to requests for information after 15 days. Our specialists will read your report and start working on it right away.

What to report - Examples of vulnerabilities could be:

- Remote Code execution
- Business Logic bypass
- Parameter Manipulation
- Cross Site scripting (XSS)
- Cross Site Request Forgery (CSRF)
- SQL injection
- Encryption vulnerabilities
- Authentication bypass, unauthorized data access

Excluded from reporting

- All reported vulnerabilities without a properly described evidence report of proof of possible exploitation
- Vulnerabilities found on sites of organizations that are no longer part of IDFC (former business units)
- Our policies on presence or absence of SPF/DKIM/DMARC records
- CSRF vulnerabilities on static pages (only on pages behind logon)/ Logout CSRF.
- Descriptive error messages (e.g. Stack Traces, application or server errors/ HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Banner disclosure on common/public services/Disclosure of known public files or directories, (e.g. robots.txt).
- Clickjacking and issues only exploitable through clickjacking.

- CSRF on forms that are available to anonymous users (e.g. the contact form).
- Presence of application or web browser 'autocomplete' or 'save password' functionality.
- Lack of Secure and HTTPOnly cookie flags/Lack of Security Speedbump when leaving the site.
- Username enumeration via Login Page error message or Forgot Password error message
- Login or Forgot Password page brute force and account lockout not enforced.
- OPTIONS / TRACE HTTP method enabled/ SSL Insecure/weak cipher suites
- SSL Attacks such as BEAST, BREACH, Renegotiation attack, SSL Forward secrecy not enabled
- The Anti-MIME-Sniffing Header X-Content-Type-Options
- Missing HTTP security headers, specifically/Redirection from HTTP to HTTPS
- HTML does not specify charset/HTML uses unrecognized charset
- Absence of using HTTP Strict Transport Security (HSTS)
- Cacheable HTTPS response pages on sites that do not provide user details or money transfer capabilities
- User enumeration on sites that do not provide money transfer capabilities
- Server or third party application version revealed and possible outdated without Proof of Concept on the exploitation of it
- Reports of insecure SSL/TLS ciphers and other misconfigurations
- Generic vulnerabilities related to software or protocols not under control of IDFC
- Findings from physical testing such as office access (e.g. open doors, tailgating).
- Findings derived primarily from social engineering (e.g. phishing, vishing).
- Functional, UI and UX bugs and spelling mistakes.
- Network level Denial of Service (DoS/DDoS) vulnerabilities
- Reports of regular scans like Port scanners
- Do not use brute force techniques, such as repeatedly entering passwords, to gain access to systems.

Reward

To encourage reporting vulnerabilities to IDFC, we would urge you to send any vulnerabilities you detect to us. As mentioned, you may receive a reward. The amount of the reward depends on the severity of the vulnerability reported, the type of website (static information sites versus online banking sites) concerned and the quality of the report we receive. If the report is of great value for the continuity and reliability of the bank, the reward will be considerably higher.

Rewards will be declined if we find evidence of abuse.