

---

## Responsible Disclosure Policy

**Terms of responsible disclosure: A right responsible disclosure approach by an individual ensures security bugs and any other security related concerns observed in Niyogo Information System and associated infrastructure are communicated directly to the Niyogo as per the details provided within this page.**

*This Page was last updated on 29th Sept 2020.*

Niyogo takes security bugs seriously to ensure Privacy & Security of users and for this reason Niyogo as a security aware organization has introduced a responsible disclosure program for reporting of any security bugs which you as a visitor or a registered user may encounter while exploring our website and/or services at any point of time.

As a security aware organization, we strongly feel there is always scope of improvement. If you come across any bugs in our Information System then you can directly reach out to us at [security-ops@goniyo.com](mailto:security-ops@goniyo.com) with details; we assure you that we will take any security specific bug-report seriously and will also update you on its progress with a thanks note directly from management of Niyogo.

Please note, currently Niyogo do not authorise posting of Bugs associated with Niyogo Information System on any forums, blog, social media etc. Also, Niyogo do not encourage researcher or ethical hacker to perform any automated or manual scan without formal engagement & authorisation against any of the Information System associated with Niyogo and thus consider any such attempt as unauthorised act and violation of related laws and regulations which includes but not limited to Section 43 and Section 66 of IT Act 2000 (amended via 2008).

Hence it is advised to follow the terms of responsible disclosure and process as specified by Niyogo for reporting any security bugs.

Thanks for helping us in improving security of our Information System and to make the web a safer place to be.

### **Process of reporting bugs:**

1. Specify Subject with details type of Bugs (i.e. Security, Privacy, Phishing, Error etc..)
2. Mark directly to "security-ops@goniyo.com". Please ensure no other email is marked in CC.
3. It is encouraged to use your own system to send bug details, please avoid using open proxy, VPN or tor network.

### **FAQ:**

**Q: What all things I can report to [security-ops@goniyo.com](mailto:security-ops@goniyo.com) ?**

A: You may report any bugs in relation to user experience, unexpected error and any issues which you see as Privacy & Security concern.

You can also report any rogue or phishing website, phishing email, sms phishing (SMiShing) and voice phishing (Vishing) associated with the Niyo brand.

If you suspect you already provided sensitive information to scammers on Call/SMS/Email/Website such as Card details, PIN, ID, Password or any other information related to Niyo, than you may report the incident directly to our customer support or write to us immediately.

**Q: Is it authorised to perform vulnerability scanning on any of the infrastructure associated with Niyo ?**

A: No, not as on date. Niyo currently don't authorise any vulnerability assessment and related activities against its infrastructure without formal engagement; only authorised consultant and researcher with Non-disclosure Agreement in place can scan the Niyo infrastructure for approved period as per agreement.

**Q: Is it authorised to make a public post about the bugs I have discovered and/or reported on Niyo Information System?**

A: No, currently Niyo do not authorise posting of Bugs associated with Niyo information System on any forums, blog, social media etc.

**Q: What are considered as unauthorised act and what are its implications?**

A: Any unauthorised attempt of identifying vulnerability in any part of Niyo Information Infrastructure will be considered as an unauthorised act. Unauthorised act include but are not limited to scanning, hacking attempts, source code theft, disclosure of confidential information, hosting phishing page, phishing scam and Identity impersonation of Niyo personnel.

An unauthorised act may attract appropriate disciplinary action at the sole discretion of the management and civil & criminal liabilities as applicable.

**Q: Is there any associated reward for reporting bugs or Niyo has a plan to introduce one in future?**

A: Currently Niyo is not involved in offering bug bounty however it is in the roadmap of Niyo; Launch of such program will be announced officially through an update on this page.

*\* Information System in this Policy refers to Mobile Application, Web Application, Websites, Servers, Services, Domains, IP Address and associated infrastructure where Niyo stores or process any information and/or data.*