Introduction

ZeroDay Alliance is the primary cybersecurity club of Sister Nivedita University (SNU). It serves as the central hub for all major cybersecurity-related activities within the institute, fostering a vibrant community of security enthusiasts and innovators across departments.

Mission

To empower students and enthusiasts in cybersecurity through inclusive learning, hands-on experiences, and collaborative challenges—fostering the skills and mindset required to identify, defend against, and innovate around digital threats.

Vision

To become a dynamic hub of cyber-defenders and innovators who transform curiosity into capability, shaping a safe, resilient digital ecosystem where every community member contributes to advancing security knowledge and practice.

Foundation date

Sep 5, 2024

Events conducted

Cybersecurity & Cloud Computing

Aug 14, 2024, Aug 22, 2024
A two-part session on securing cloud environments, cloud threats, and industry security practices.

Official Club Orientation

Sep 5, 2024
This offline event marked the official introduction of the ZeroDay Alliance to the student community. The orientation session was aimed at familiarizing students with the club’s

vision, mission, and upcoming initiatives. With strong academic support from distinguished faculty members, the event successfully ignited interest among students across multiple disciplines, promoting a culture of cybersecurity awareness and collaboration.
Event Photos: Official Club Orientation

Cybersecurity for Beginners

Oct 6, 2024
This online educational session served as an excellent starting point for students interested in cybersecurity. Designed specifically for beginners, the session aimed to build awareness about the evolving cyber threat landscape and emphasized the importance of fundamental security practices. The event provided students with a solid foundation to explore cybersecurity as a potential career path.

Basics of Operating System

Oct 20, 2024
A beginner-friendly session explaining Operating System (OS) fundamentals, including process management, memory management, and security vulnerabilities, forming the essential base for students aspiring towards cybersecurity and system-level learning.

Team: Blue

Oct 23, 2024
The seminar focused on critical aspects of cybersecurity defense, introducing students to core blue team operations such as security monitoring, incident response strategies, and proactive defense mechanisms.

Introduction of Computer Networks

Aug 27, 2024
Description: The session provided an introduction to the fundamentals of computer networks, focusing on key concepts like TCP/IP architecture, subnetting, and basic network security principles.

403 – Permission Denied

Nov 9, 2024
A hands-on seminar aimed at introducing students to ethical hacking and penetration testing, with live demonstrations of real-world cybersecurity techniques.
Event Photos: 403 – Permission Denied

Bug Hunt 404

Jan 6, 2025
An educational seminar focused on introducing students to the world of bug bounty hunting, vulnerability research, and responsible disclosure practices.

Securing Generative AI - Risk and Strategies

Jan 19, 2025
This collaborative event with SKEPSIS introduced the participants to the emerging field of Generative AI and the cybersecurity risks associated with it. The session was designed to bridge the gap between innovation in AI and the security challenges that arise from its applications. Attendees explored fundamental concepts of AI, potential threats, and basic mitigation strategies, gaining an essential understanding of the need for security in modern AI systems.
Event Photos: Securing Generative AI - Risk and Strategies

Cybersecurity for AI Professionals

Feb 19, 2025
This offline seminar aimed to introduce attendees to the intersection of Artificial Intelligence and Cybersecurity, emphasizing the growing importance of AI-driven defense strategies. Organized solely, the event focused on building awareness about information security principles, emerging cybersecurity trends, and lucrative career pathways for AI and cybersecurity enthusiasts.
Event Photos: Cybersecurity for AI Professionals

Phantom Breach - Capture The Flag (CTF)

Apr 17, 2025
This offline Capture The Flag (CTF) Competition was organized in collaboration with the GNIT Cybersecurity Club at Guru Nanak Institute of Technology, Panihati. The competition aims to test cybersecurity skills, teamwork, and problem-solving abilities. Students from various technical backgrounds registered enthusiastically, showing a growing interest in hands-on cybersecurity challenges and real-world vulnerability solving.
Event Photos: Phantom Breach CTF

0th Day

Sep 13, 2025
This was an exclusive session for the freshmen of SNU where we unveiled our vision and future roadmap of ZeroDay Alliance to them. We gave them an opportunity to interact with us and discover why ZDA stands apart, explore our past achievements, and see how we’re gearing up for the next era of cybersecurity excellence.
Event Photos: 0th Day

Virtual Lab Setup: A Practical Guide

Oct 26, 2025
In this session, ZeroDay Alliance guided students through the secure installation of Virtual Machines and Linux environments on their systems. Participants learned the fundamentals of cybersecurity exploration, Linux operations, and the ethical guidelines essential for responsible cyber practices. This workshop empowered attendees to confidently navigate

and experiment within safe, virtualized environments – marking their first step into the cybersecurity domain.

Website

zerodayalliance.tech

Social Media pages

Instagram: @zerodayalliance
Linkedin: company/zeroday-alliance
X (Twitter): @zerodayalliance
YouTube: @zerodayalliance
GitHub Organization: @zerodayalliance

Members of 2025–26 tenure

President

Avik Samanta

Vice Presidents

Adrija Ghosal
Praveen Joshi

Tech Teams

Cybersecurity Team:

Vinit Kumar Singh [**Lead**]

- Adrija Karmakar
- Aman Kumar Rai
- Anant Gupta
- Anindita Sarkar
- Anuska Roy
- Prithwish Ghosh
- Ritam Parui

DevOps Team:

Krishnendu Das [**Lead**]

- Snigdha Mistry

Web Development Team:

Krishnendu Das [**Lead**]

- Agnik Mukherjee
- Ayush Ghosh
- Eshani Paul
- Subham Majumdar

Non-Tech Teams

Design Team:

Sinjini Ghosh [**Lead**]

- Aayushman Bhardwaj
- Sneha Kundu
- Sneha Mandal
- Sourik Sasmal
- Subham Dey

Social Media & Content Team:

Soumyajyoti Guha [**Lead**]

- Arpan Roychowdhury
- Dipta Sundar Dutta
- Nilanjan Dutta
- Shakshi Kumari Shaw
- Sk. Afif Hassan

PR & Outreach Team:

Sneha Karmakar [**Lead**]

- Ananya Priya
- Yashvi Dubey

Event Management Team:

Shekhar Shubham Thakur [**Lead**]

- Argha Ranjan Singha
- Sayani Rana
- Sayoni Chakraborty
- Soumili Saha

Rules & Regulations

This manual governs the functioning of ZeroDay Alliance under the Department of Computer Science & Engineering, Sister Nivedita University. It aims to ensure smooth administration, promote decentralization, and standardize procedures for club management.

1. Formation

1.1. No duplicate club or chapter of the same organization shall be permitted within the department.

1.2. Club leads are not allowed to lead multiple clubs without prior approval from ZeroDay Alliance.

1.3. The club shall not charge any joining or membership fee unless explicitly permitted by the Faculty Point of Contact (POC).

2. Functioning

2.1. Events organized by any club must not overlap with those of other clubs. Proper coordination must be maintained to ensure fair scheduling across all clubs.

2.2. Participation in any event shall remain voluntary unless specifically mandated by the Faculty POC.

2.3. All events, collaborations, and external engagements must align with the policies of Sister Nivedita University.

3. Objectives & Activities

3.1. The primary objective of ZeroDay Alliance is to promote learning, collaboration, and innovation within the field of cybersecurity.

3.2. The club shall organize lectures, workshops, seminars, CTFs and industry interactions to enhance members' technical knowledge and professional exposure.

3.3. The club shall actively support students in:

- 3.3.1. Developing technical and soft skills
- 3.3.2. Preparing for placements and competitions
- 3.3.3. Participating in social or community-driven initiatives

3.4. Focus areas may extend beyond cybersecurity to include Web Development, AI/ML, DevOps, Internet of Things (IoT), and other emerging domains that contribute to strengthening cybersecurity knowledge.

4. Structure

4.1. Faculty POCs: 2

4.2. President: 1

4.3. Vice Presidents: up to 2

4.4. Core Members: up to 45

5. Core membership

5.1. Membership is open to all active or recently graduated students of Sister Nivedita University, regardless of major or department.

5.2. Membership shall remain free of cost.

5.3. Applicants for each tenure must undergo a mandatory interview, conducted by outgoing club leads and relevant team leads, to qualify for membership.

5.4. Members are free to join multiple clubs across the university.

5.5. Members found acting against the objectives or code of conduct of the club may be removed by the club leads, based on recommendations from the concerned team lead(s).

6. Administration

6.1. All activities of ZeroDay Alliance must strictly adhere to university guidelines.

6.2. The club reserves the right to appoint, replace, or restructure executive members as deemed necessary.

6.3. Past senior members may be appointed as mentors to guide and advise new members and leads; however, mentors shall not hold any executive powers.

7. Selection & Tenure

7.1. Leads for each new tenure shall be selected through a mutual voting process among existing leads and team leads, following an interview of each applicant.

7.2. The selected leads must receive final approval from the Faculty POC.

7.3. The selection of club leads must be completed by 31st August each year.

7.4. Each tenure shall commence on 1st September and conclude on 31st July of the following year.

7.5. Membership or leadership positions shall not be automatically renewed; individuals must reapply and undergo the selection process for each new tenure.

8. Code of Conduct

8.1. All members are expected to maintain respect, professionalism, and integrity in every interaction.

8.2. Bullying, harassment, disrespect, or unauthorized promotions of any kind are strictly prohibited.

8.3. Members must report any disputes, grievances, or issues directly to the leads or Faculty POC.

8.4. Violations of the code of conduct may result in suspension, demotion, or expulsion, based on the severity of the misconduct.

8.5. The Faculty POC holds the final authority in all disciplinary matters.