

Dayanand Science College Latur Maharashtra

IT-Cyber Security Policy

INFORMATION TECHNOLOGY-CYBER SECURITY POLICY

This cyber security policy is for our faculties, administrative staff, students, employees, vendors and partners to refer to when they need advice and guidelines related to cyber law and cybercrime. Having this cyber security policy, we are trying to protect and promote the secure data and technology infrastructure of Dayanand Science College, Latur.

Scope

This policy applies to all of institution's students, faculties, administrative staff, other employees, contractors, volunteers, vendors, collaborators and anyone else who may have any type of access to institution's systems, software and hardware.

Confidential Data

- Some of the common examples of confidential data include:
- Student personal data
- Faculty personal data
- Classified Data pertained to Controller of Examinations
- Data about partners
- Data about vendors
- Patents, formulas or new technologies
- Classified financial information

Device Security – Using personal devices

Logging in to any of institution's accounts for personal devices such as mobile phones, tablets or laptops, can put our institution's data at risk. Dayanand Science College Latur, does not recommend accessing any institutional data from personal devices. If so is inevitable, stakeholders are obligated to keep their devices in a safe place, not exposed to anyone else.

We recommend stakeholders to follow these best practices:

- Keep all electronic devices' password secured and protected
- Logging into institution's accounts should be done only through safe networks
- Install security updates on a regular basis
- Upgrade antivirus software on a regular basis
- Don't ever leave your devices unprotected and exposed
- Lock your computers when leaving the desk

Email Security

Emails can carry scams or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, our policy is always to inform stakeholders to:

- Abstain from opening attachments or clicking any links in the situations when its content is not well explained
- Make sure to always check email addresses and names of senders.
- Search for inconsistencies
- Be careful with malwares, clickbait titles (for example offering prizes, advice, etc.)
- Change all account passwords at once when a device is stolen.
- In case that a student/faculty/employee/office is not sure if the email received, or any type of data is safe, they can always contact our IT specialist.

Managing Passwords

To ensure avoiding that your institution account password gets hacked, use these best practices for setting up passwords:

- At least 8 characters (must contain capital and lower-case letters, numbers and symbols)
- Do not write down password and leave it unprotected
- Do not exchange credentials when not requested or approved by supervisor
- Change passwords every 2 months

Transferring Data

Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

- Avoid transferring personal data such as student and employee confidential data
- Adhere to personal data protection law
- Data can only be shared over institution's network
- Our Network Administrators / Security Specialists should:
- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all faculties and students.
- Inform stakeholders regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow the provisions of this policy as other stakeholders do.
- Even when working remotely, all the cyber security policies and procedures must be followed.

Disciplinary Action

We expect all our stakeholders to always follow this policy and those who cause security breaches may face disciplinary action. Some of the examples of disciplinary actions include:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause any sort of damage): We will invoke more severe disciplinary action up to and including termination.
- Each case and incidence will be assessed on a case-by-case basis.
- Everyone who disregards institution's policies will face progressive discipline.


Consultancy Policy

GET IN TOUCH WITH US!

Dayanand Science College, Latur, Maharashtra, India

Phone: +91 2382 221149


IQAC Coordinator
Dayanand Science College,
Latur, M.S. (INDIA)


Principal
PRINCIPAL
Dayanand Science College
LATUR