



Cyber Security and Data Privacy Policy

We at UltraTech Cement Limited recognise the importance of cyber security and data privacy in delivering seamless information services to enable business operations, enhance productivity, customer satisfaction and stakeholder value along with adequate protection of information assets.

We are committed to establish and improve cyber security preparedness and minimise its exposure to associated risks. All businesses and functions of UltraTech Cement will implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

To achieve this, we shall:

- Comply with applicable national and international cyber-security norms and standards.
- Classify information assets based on their business value and risk exposure.
- Provide necessary measures such as Policy, Procedure, and appropriate solutions through Information Security Management System (ISMS) framework, aligned to business requirement.
- Continuously strive to improve and strengthen our Information Security initiatives through identification of cyber risks and mitigation to acceptable level.
- Protect our stakeholders, critical information and assets from threats that could potentially disrupt business and our brand reputation.
- Design, Develop and Implement highly secure and highly available IT Systems to facilitate smooth business operations.
- Optimise, enhance and align IT Services to changing business needs in terms of IT Infrastructure and Application.
- Conduct regular cyber-security audits following appropriate national and international standards to maintain compliance.
- Collaborate with cyber-security and data privacy experts to continually enhance cyber-security framework.
- Communicate importance of cyber-security to all stakeholders and continually enhance their information security awareness.
- Establish clear-cut reporting channels for any form of violation of the cyber-security and data privacy policies.
- Investigate cyber-security incidents that comes to our notice and initiate appropriate corrective and preventive actions.

This policy shall be made available to employees and other concerned parties.

The content and implementation of this policy shall be reviewed and updated periodically, synchronized to changing IT landscape.
