DISCLAIMER & POLICIES

DISCLAIMER

The information provided on this website is for general informational purposes only. **The Maharashtra Housing and Area Development Authority (MHADA)** makes every effort to ensure the accuracy and reliability of the information presented; however, we do not guarantee its completeness, correctness, or timeliness.

MHADA shall not be held responsible for any errors, omissions, or inaccuracies in the content or for any loss or damage arising from reliance on the information provided on this website. Users are advised to verify the information with the relevant MHADA department before making any decisions or taking any actions.

This website may contain links to external websites for user convenience. MHADA does not endorse, control, or take responsibility for the content, policies, or practices of any third-party websites.

All materials on this website, including text, graphics, logos, and images, are the property of MHADA unless otherwise stated. Unauthorized reproduction, modification, or distribution of any content is strictly prohibited.

By accessing and using this website, users agree to comply with the terms outlined in this disclaimer. MHADA reserves the right to modify or update the content and policies without prior notice.

For official information, users are encouraged to contact MHADA directly through its designated communication channels.

COPYRIGHT & INTELLECTUAL PROPERTY POLICY

Unless otherwise indicated, all content on this website—including text, images, graphics, logos, audio, video, software, and other material—is the intellectual property of MHADA and is protected by applicable copyright and intellectual property laws of India.

Reproduction, redistribution, republication, or transmission of material from this website is permitted without prior approval only if:

- The material is used for non-commercial, informational, and personal purposes.
- The material is not altered, misrepresented, or used in a misleading context.
- Proper attribution to MHADA is provided.

Content identified as third-party copyright remains the property of the respective owners. Permission for use of such content must be obtained directly from the concerned copyright holder.

CONTENT CONTRIBUTION, MODERATION AND APPROVAL POLICY (CMAP)

Content is created by the Nodal officers designated by the Web Information Manager. It is approved by the Web Information Manager and emailed to ictcell@mhada.gov.in for publishing on the website of MHADA. We also ensure that the website content is free from offensive and/or discriminatory language.

Content received by the webmaster on the designated email ID ictcell@mhada.gov.in is published on the website through a web-based Content Management System within the same working day.

Sr. No.	Content Element	Frequency	Reviewer	Approver
1	Banners on Homepage	Half yearly	Nodal Officer	Web Information Manager
2	Banners on internal pages	Half yearly	Nodal Officer	Web Information Manager
3	Disclaimer and Policies	Yearly	Nodal Officer	Web Information Manager

4	Accessibility statement	Yearly	Nodal Officer	Web Information Manager
5	Help	Yearly	Nodal Officer	Web Information Manager
6	Feedback	Yearly	Nodal Officer	Web Information Manager
7	Contact Us	Yearly	Nodal Officer	Web Information Manager

CONTENT REVIEW POLICY

Website content is reviewed periodically for accuracy, relevance, and grammar by designated nodal officers and the Web Information Manager.

Expired or outdated content such as tenders, notices, or announcements shall be removed or archived in accordance with defined archival procedures.

Essential static pages such as “About Us,” “Services,” “Contact Us,” and “Disclaimer” shall be reviewed annually or as required.

The entire website content is reviewed for syntax/grammar checks once in a month by the Web Information Manager.

Sr. No.	Tab heading	Frequency of review	Reviewer	Approver
1	About Us	Yearly	Nodal Officer	Web Information Manager
2	Emergencies	Yearly	Nodal Officer	Web Information Manager
3	Services	Monthly	Nodal Officer	Web Information Manager

HYPERLINKING POLICY

a) Links to External Sites: This website may contain links to external government and non-government websites. MHADA is not responsible for the content, accuracy, or reliability of linked websites and does not endorse the views expressed therein.

b) Links to MHADA Site: Direct linking to pages or documents hosted on the MHADA website is permitted without prior permission, provided such links do not misrepresent MHADA's role or load the content within frames. MHADA content must always open in a separate browser window.

PRIVACY POLICY

MHADA respects the privacy of all visitors to this website. As a general rule, the website does not automatically collect any personal information such as name, phone number, or email address.

Standard information collected automatically includes Internet Protocol (IP) addresses, browser type, operating system, pages visited, and date/time of access. This information is collected solely for statistical and security purposes and does not identify individual users.

Personal data provided voluntarily by users (e.g., through forms, applications, or feedback) will be used only for the stated purpose and shall not be shared with third parties, except when disclosure is required under law or to protect MHADA's rights.

MHADA employs reasonable administrative, technical, and physical safeguards to protect user information. However, MHADA does not guarantee that such information will never be subject to unauthorized access, disclosure, or misuse.

TERMS AND CONDITIONS

By accessing and using this website, users agree to comply with and be legally bound by these terms and policies under the applicable laws of India.

Users shall not engage in unauthorized activities such as hacking, uploading harmful material, misrepresentation, or any illegal use of this website.

MHADA does not guarantee that the website will always be available, uninterrupted, or error-free. Temporary suspension of access may occur due to maintenance, upgrades, technical issues, or circumstances beyond MHADA's control.

Information contained herein shall not be treated as a statement of law and cannot be relied upon for legal purposes. Users are advised to consult appropriate legal or professional advisors for specific queries.

WEBSITE MONITORING PLAN

Website Monitoring Policy is in place and the website is monitored periodically to address and fix the quality and compatibility issues around the following parameters:

Performance: Site download time is optimized for a variety of network connections as well as devices. All important pages of the website are tested for this.

Functionality: All modules of the website are tested for their functionality. The interactive components of the portal such as feedback forms are working smoothly.

Broken Links: The portal is thoroughly reviewed to rule out the presence of any broken links or errors.

Traffic Analysis: The site traffic is monitored to analyse the usage patterns as well as visitors.

Feedback: A proper mechanism for feedback is in place to carry out the changes and enhancements as suggested by the visitors.

CONTINGENCY MANAGEMENT PLAN

A contingency plan is crucial to ensure preparedness and minimize the impact of defacement or natural calamities. Here are some general steps we considered while developing a contingency plan:

Risk Assessment: We have identified the potential risks and vulnerabilities our organization may face, such as defacement of property or natural calamities like floods, earthquakes, storms, or fires. We have assessed the likelihood and potential impact of each risk.

Emergency Response Team: We have established an emergency response team comprising key personnel from different departments. We have defined their roles and responsibilities in the event of an emergency. We have also designated a team leader who will coordinate the response efforts.

Communication Plan: We have established a clear communication plan to ensure effective communication with employees, stakeholders, and the public. This plan includes multiple channels of communication, such as email, text messages, social media, and designated communication points.

Data Backup and Recovery: We regularly backup critical data and store it securely in the cloud. We have established a data recovery plan to ensure the restoration of essential systems and data in the event of defacement or data loss.

Physical Security Measures: We have implemented security measures to protect our organization's assets, including surveillance systems, access controls, and alarms. We have also considered measures to protect against vandalism or defacement.

Training and Drills: We regularly conduct training sessions and emergency drills to educate employees about emergency procedures and their roles during an emergency. These drills help ensure that everyone is prepared and familiar with the contingency plan.

Recovery and Restoration: We have developed strategies for post-event recovery and restoration of normal operations. We have identified key priorities, such as damage assessment, repairs, resuming essential services, and supporting affected employees.

Regular Plan Review and Updates: We continuously review and update our contingency plan to incorporate lessons learned from drills, real events, or changes in the organization's structure or operations. We also ensure that the plan remains current and relevant.

BUSINESS CONTINUITY PLAN

Developing a business continuity plan (BCP) specific to organization involves a thorough understanding of operations, critical processes, and potential risks. Here are some key steps we have considered to create a business continuity plan:

Business Impact Analysis (BIA): We have conducted a comprehensive assessment of our organization's critical functions, processes, and dependencies and identified potential risks, determined the impact of disruptions on our operations, such as financial loss, reputational damage, and customer dissatisfaction.

Risk Assessment: We have evaluated the risks specific to our organization, including natural disasters, cyber threats, supply chain disruptions, and any other potential hazards and prioritized the risks based on their likelihood and impact on our business.

Recovery Objectives: We have determined the recovery time objectives (RTO) and recovery point objectives (RPO) for each critical process. RTO defines the acceptable downtime for a process, while RPO determines the maximum data loss permissible.

Continuity Strategies: We have developed strategies to mitigate the impact of disruptions and ensure continuity of operations. This includes redundant systems, alternative suppliers, backup facilities, cloud-based services, and remote work arrangements. We have considered the costs, feasibility, and effectiveness of each strategy.

Emergency Response Plan: We have established an emergency response team and defined their roles and responsibilities during an emergency. We have created a clear communication plan to ensure effective internal and external communication during the crisis. We have also identified primary and alternate means of communication.

Data Backup and Recovery: We have implemented a robust data backup and recovery system. We regularly backup critical data and ensure secure offsite storage or cloud-based solutions. We also test data recovery procedures to ensure data integrity and availability.

Incident Management: We have developed procedures to identify, report, and respond to incidents promptly. We have established protocols for escalation, decision-making, and coordination during an emergency and trained employees on incident management processes and their roles.

Testing and Training: We regularly conduct BCP drills and exercises to test the effectiveness of the plan. We identify gaps or areas for improvement and update the plan accordingly. We also provide training to employees on their roles and responsibilities during an emergency.

Plan Maintenance and Review: We continuously review and update our business continuity plan as our organization evolves or new risks emerge. We keep contact lists, emergency procedures, and recovery strategies up to date. We also conduct periodic audits to ensure compliance with the plan.

DEFACEMENT OF THE WEBSITE UNDER BUSINESS CONTINUITY PLAN

Addressing the defacement of a website as part of a business continuity plan involves specific steps to restore the website's functionality, reputation, and security. Here is the approach we have for dealing with website defacement:

Detection and Response:

We monitor our website regularly to detect any signs of defacement. Implement security measures like intrusion detection systems and web application firewalls to aid in early detection.

As soon as defacement is detected, we trigger our incident response plan and notify our designated response team.

We assess the extent of the defacement and gather evidence. Take screenshots or capture the defaced pages for documentation purposes.

Isolate and Investigate:

We immediately isolate the affected website to prevent further damage or compromise.

We conduct a thorough investigation to determine the cause and extent of the defacement. Identify any potential vulnerabilities or weaknesses in our website's security.

Restore from Backup:
We initiate the restoration process from a known backup that predates the defacement. Ensure that the backup is clean and free from any malicious code or vulnerabilities.

We verify the integrity of the backup and validate that the restored website is functioning correctly.

Patch and Secure:

We identify and address any vulnerabilities or weaknesses that led to the defacement. Update our website's software, plugins, themes, and any other components to their latest versions.

We implement robust security measures, such as strong authentication mechanisms, regular security audits, and web application firewalls, to safeguard against future defacement attempts.

Review and Test:

We conduct a thorough review of the incident and identify any lessons learned. Assess the effectiveness of our response and recovery efforts.

We perform penetration testing or vulnerability assessments to identify and address any remaining security gaps.

Regularly test our website's security and functionality to ensure ongoing protection against defacement or other threats.

Communication and Reputation Management:

We have developed a communication plan to inform our stakeholders, customers, and users about the incident, the steps taken to address it, and any measures implemented to prevent future incidents.

We are transparent and proactive in addressing any concerns or questions raised by stakeholders.

We monitor our website's reputation and respond promptly to any negative impact resulting from the defacement. We engage in public relations activities as necessary to restore trust and confidence.

DATA CORRUPTION AS PER DR

Resolving data corruption from a Disaster Recovery (DR) site involves a systematic approach to restore data integrity and ensure business continuity. Here are the general steps to address data corruption from a DR site:

Identify and Isolate Corrupted Data:

Determine the scope and extent of the data corruption. Identify the specific files, databases, or systems affected by the corruption.

Isolate the corrupted data to prevent further damage or spreading of the corruption. This involve disconnecting affected systems from the network or disabling access to corrupted files.

Determine the Source and Cause:

Investigate the cause of the data corruption. It could be due to hardware failures, software bugs, human error, malware, or other factors.

Determine whether the corruption originated from the primary site or occurred during the replication process to the DR site. This information helps in identifying the appropriate resolution steps.

Restore from Backup:

With clean backups of the affected data, initiate the restoration process from a known good backup. Ensure that the backup is unaffected by the data corruption.

Verify the integrity of the backup and validate the restored data to ensure it matches the expected state.

Data Synchronization and Reconciliation:

If the data corruption occurred during replication to the DR site, initiate a synchronization process to reconcile the corrupted data.

Depending on the replication method and technologies used, consult the documentation or contact the vendor for guidance on how to synchronize and resolve any discrepancies.

Data Repair and Recovery:

In cases where the corrupted data cannot be restored from backups or synchronization alone, consider data repair techniques. This involve using specialized tools or engaging data recovery experts to salvage and repair the corrupted data.

Data Validation and Testing:

Once the data restoration and repair processes are complete, validate the integrity and accuracy of the recovered data. Perform thorough testing and verification to ensure that the data is usable and free from corruption.

System and Process Improvements:

Analyse the root cause of the data corruption incident and identify any underlying vulnerabilities or weaknesses in systems or processes.

Implement appropriate measures to prevent future data corruption incidents. This involve hardware upgrades, software patches or updates, improved backup and replication procedures, or enhanced data validation checks.

Documentation and Communication:

Document the steps taken to resolve the data corruption issue, including the root cause analysis and the actions performed to recover the data.

Communicate with relevant stakeholders, such as IT teams, management, and affected users, to keep them informed about the incident, resolution, and any preventive measures implemented.

NATURAL DISASTERS ACCORDING TO DR AND DC AND VICE VERSA

DR (Disaster Recovery) and DC (Data Centre) are closely related concepts, and they both play critical roles in mitigating the impact of natural disasters on business operations. Here's an overview of how they relate to each other:

Disaster Recovery (DR):

DR refers to the strategies, processes, and procedures put in place to recover and restore critical business functions and IT systems after a disruptive event, such as a natural disaster.

A DR plan outlines the steps to be taken to minimize downtime, recover data, and resume operations in the event of a disaster.

DR typically involves maintaining redundant systems, data backups, and alternate infrastructure at an off-site location to ensure business continuity.

Data Centre (DC):

A data centre is a physical facility that houses computer systems, servers, networking equipment, and storage resources required for processing and storing data.

Data centres are designed to provide a controlled and secure environment for housing critical IT infrastructure.

They include redundant power supplies, cooling systems, fire suppression measures, and physical security measures to protect the equipment and ensure uninterrupted operation.

Interconnection between DR and DC in the context of natural disasters.

WEBSITE SECURITY POLICY

MHADA employs secure servers and reasonable security measures, including monitoring of network traffic, to safeguard the integrity of data and prevent unauthorized access.

Attempts to upload or alter information, defeat security measures, or cause harm to the website are strictly prohibited and subject to prosecution under relevant IT and cyber laws of India.

In case of detected breaches, MHADA may share relevant information with law enforcement authorities for investigation and prosecution.

Web Information Manager

Name: Sandeep Bodele, ICT Officer

Contact: 022-66405000