

अस्वीकरण आणि धोरणे

अस्वीकरण

या संकेतस्थळावर दिलेली माहिती ही केवळ सामान्य माहितीपुरती असून ती सर्वसामान्यांच्या माहितीसाठी उपलब्ध करून दिलेली आहे. महाराष्ट्र गृहनिर्माण व क्षेत्रविकास प्राधिकरण (म्हाडा) येथे सादर करण्यात आलेली माहिती अचूक व विश्वासाह राहावी यासाठी सर्वतोपरी प्रयत्न करते; तथापि, या माहितीची पूर्णता, बरोबरी किंवा अद्ययावतपणा याची हमी देत नाही.

या संकेतस्थळावरील माहितीवर अवलंबून राहिल्यामुळे किंवा तिच्या वापरामुळे उद्भवणाऱ्या कोणत्याही चुका, त्रुटी, अचूकतेतील त्रुटी तसेच झालेल्या नुकसानीबाबत म्हाडा जबाबदार राहणार नाही. कोणतेही निर्णय घेण्यापूर्वी किंवा कृती करण्यापूर्वी वापरकर्त्यांनी संबंधित म्हाडा विभागाकडून माहितीची खात्री करून घ्यावी.

या संकेतस्थळावर वापरकर्त्यांच्या सोयीसाठी बाह्य संकेतस्थळांच्या दुव्यांचा समावेश असू शकतो. त्या तृतीय पक्षाच्या संकेतस्थळांवरील मजकूर, धोरणे किंवा पद्धती याबाबत म्हाडा ना समर्थन करते, ना नियंत्रण ठेवते, ना जबाबदारी स्वीकारते.

या संकेतस्थळावरील सर्व साहित्य, ज्यामध्ये मजकूर, चित्रमय माहिती, लोगो आणि प्रतिमा यांचा समावेश आहे, ते अन्यथा नमूद केलेले नसल्यास म्हाडाची मालमत्ता आहे. या मजकुराचे अनधिकृत पुनरुत्पादन, बदल अथवा वितरण करण्यास सक्त मनाई आहे.

या संकेतस्थळाचा वापर करून व त्यास प्रवेश करून वापरकर्ते या अस्वीकरणातील अटी मान्य करतात. म्हाडा यामधील मजकूर व धोरणे कोणतीही पूर्वसूचना न देता बदलण्याचा किंवा अद्ययावत करण्याचा अधिकार राखून ठेवते.

अधिकृत माहितीसाठी वापरकर्त्यांनी म्हाडाशी त्याच्या निर्दिष्ट संवाद माध्यमांद्वारे थेट संपर्क साधावा.

कॉपीराइट व बौद्धिक संपदा धोरण

अन्यथा नमूद केल्याशिवाय, या संकेतस्थळावरील सर्व मजकूर, चित्रे, ग्राफिक्स, लोगो, ध्वनी, व्हिडिओ, सॉफ्टवेअर आणि इतर साहित्याचा बौद्धिक संपदा हक्क म्हाडा कडे आहे आणि ते भारतातील लागू असलेल्या कॉपीराइट व बौद्धिक संपदा कायद्यांद्वारे संरक्षित आहे. साहित्याचे पुनरुत्पादन, पुनर्वितरण, पुन्हा प्रकाशित करणे किंवा प्रसारण करण्यास पूर्व परवानगीशिवाय केवळ खालील अटींवर अनुमती आहे:

- साहित्याचा वापर गैर-व्यावसायिक, माहितीपर व वैयक्तिक उद्देशासाठी केला गेला पाहिजे.
- साहित्यामध्ये बदल, चुकीचे सादरीकरण अथवा दिशाभूल करणाऱ्या संदर्भात वापर होऊ नये.
- म्हाडा ला योग्य श्रेय दिले जावे. तृतीय-पक्षांच्या कॉपीराइट असलेल्या सामग्रीचा मालकीहक्क त्यांच्या संबंधित मालकांकडे राहतो. अशा सामग्रीचा वापर करण्यासाठी थेट त्यांच्याकडून परवानगी घेणे आवश्यक आहे.

सामग्री योगदान, परीक्षण व मंजूरी धोरण (CMAP)

सामग्रीची निर्मिती नामनिर्दिष्ट नोडल अधिकारी करत असून ती वेब माहिती व्यवस्थापक (Web Information Manager) मंजूर करतात. मंजूर सामग्री ictcell@mhada.gov.in या अधिकृत ईमेलवर पाठवून म्हाडा च्या संकेतस्थळावर प्रकाशित केली जाते. आम्ही याचीही खात्री करतो की संकेतस्थळावरील मजकूरात आक्षेपार्ह अथवा भेदभावपूर्ण भाषा नसावी.

नियुक्त केलेल्या ईमेल आयडी **ictcell@mhada.gov.in** वर वेबमास्टरकडे प्राप्त झालेला सामग्री वेब-आधारित कंटेंट मॅनेजमेंट सिस्टिमद्वारे त्या समान कार्यदिवसात संकेतस्थळावर प्रकाशित केला जातो.

पुनरावलोकन वारंवारता

क्र.	सामग्री घटक	वारंवारता	पुनरावलोकनकर्ता	मंजूरकर्ता
१.	मुख्य पृष्ठावरील बॅनर्स	सहामाही	नोडल अधिकारी	वेब माहिती व्यवस्थापक
२.	अंतर्गत पृष्ठावरील बॅनर्स	सहामाही	नोडल अधिकारी	वेब माहिती व्यवस्थापक
३.	अस्वीकरण व धोरणे	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक
४.	प्रवेशयोग्यता विधान	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक
५.	मदत	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक
६.	अभिप्राय	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक
७.	आमच्याशी संपर्क साधा	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक

सामग्री पुनरावलोकन धोरण

संकेतस्थळावरील सामग्रीची अचूकता, सुसंगती व व्याकरण तपासण्यासाठी नोडल अधिकारी व वेब माहिती व्यवस्थापक नियतकालिक पुनरावलोकन करतात. कालबाह्य झालेली सामग्री (उदा. निविदा, सूचना, जाहिराती) ठरलेल्या पद्धतीनुसार काढून टाकली जाते किंवा संग्रहित केली जाते. महत्त्वाची स्थिर पृष्ठे जसे की "आमच्याबद्दल", "सेवा", "संपर्क", "अस्वीकरण" यांचे वार्षिक पुनरावलोकन केले जाते. प्रत्येक महिन्यात एकदा संपूर्ण संकेतस्थळावरील व्याकरण तपासणी केली जाते.

पुनरावलोकन वारंवारता

क्र.	टॅब शीर्षक	पुनरावलोकन वारंवारता	पुनरावलोकनकर्ता	मंजूरकर्ता
१.	आमच्याबद्दल	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक
२.	आपत्कालीन सेवा	वार्षिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक

क्र.	टॅब शीर्षक	पुनरावलोकन वारंवारता	पुनरावलोकनकर्ता	मंजूरकर्ता
३.	सेवा	मासिक	नोडल अधिकारी	वेब माहिती व्यवस्थापक

दुवे (Hyperlinking) धोरण

अ) बाह्य संकेतस्थळांचे दुवे: या संकेतस्थळावर शासकीय व गैर-शासकीय बाह्य संकेतस्थळांचे दुवे असू शकतात. म्हाडा त्यावरील मजकूर, अचूकता किंवा विश्वसनीयतेबद्दल जबाबदार नाही आणि त्यांना मान्यता देत नाही.

ब) म्हाडा संकेतस्थळाचे दुवे: म्हाडा संकेतस्थळावरील पृष्ठे अथवा दस्तऐवजांना थेट दुवे देणे परवानगी आहे, परंतु त्यातून म्हाडा ची भूमिका चुकीची दाखवली जाऊ नये व ते फ्रेममध्ये उघडले जाऊ नयेत. दुवे नेहमी स्वतंत्र ब्राऊझर विंडोमध्ये उघडले पाहिजेत.

गोपनीयता धोरण

म्हाडा या संकेतस्थळाला भेट देणाऱ्या सर्वांच्या गोपनीयतेचा सन्मान करते. सर्वसाधारणपणे, या संकेतस्थळाद्वारे नाव, दूरध्वनी क्रमांक किंवा ईमेल पत्ता यासारखी वैयक्तिक माहिती स्वयंचलितपणे संकलित केली जात नाही.

स्वयंचलितरित्या संकलित केली जाणारी माहितीमध्ये IP पत्ते, ब्राऊझरचा प्रकार, ऑपरेटिंग सिस्टम, भेट दिलेली पाने व भेटीची वेळ/तारीख यांचा समावेश होतो. ही माहिती केवळ सांख्यिकी व सुरक्षेसाठी संकलित केली जाते व ती व्यक्तीची ओळख पटवत नाही.

वापरकर्त्यांनी स्वेच्छेने दिलेली वैयक्तिक माहिती (उदा. फॉर्म, अर्ज, अभिप्राय) केवळ नमूद उद्देशासाठी वापरली जाईल व कायदेशीर कारणास्तव अथवा म्हाडा चे हक्क सुरक्षित ठेवण्यासाठी आवश्यक असल्याशिवाय तृतीय-पक्षांसोबत सामायिक केली जाणार नाही.

वापरकर्त्यांची माहिती सुरक्षित ठेवण्यासाठी म्हाडा प्रशासकीय, तांत्रिक व भौतिक उपाययोजना राबवते. तथापि, ही माहिती अनधिकृत प्रवेश, प्रकटीकरण अथवा गैरवापरास कधीही बळी पडणार नाही याची हमी दिली जाऊ शकत नाही.

अटी व शर्ती

हे संकेतस्थळ वापरताना वापरकर्ते नमूद केलेल्या अटी व धोरणांना मान्य करतात आणि भारतातील लागू कायद्यांनुसार त्यांना बांधील राहतील. अनधिकृत क्रियाकलाप जसे की हॅकिंग, हानिकारक सामग्री अपलोड करणे, चुकीचे सादरीकरण अथवा बेकायदेशीर वापर करण्यास सक्त मनाई आहे. म्हाडा संकेतस्थळ सतत उपलब्ध राहील, अडथळामुक्त राहील किंवा त्रुटीविरहित राहील याची हमी देत नाही. देखभाल, सुधारणा, तांत्रिक अडचणी किंवा म्हाडा च्या नियंत्रणाबाहेरील कारणास्तव प्रवेश तात्पुरता बंद राहू शकतो. या संकेतस्थळावरील माहिती ही कायदेशीर सल्ला म्हणून ग्राह्य धरता येणार नाही. विशिष्ट प्रश्नांसाठी वापरकर्त्यांनी कायदेशीर अथवा व्यावसायिक सल्लागारांचा सल्ला घ्यावा.

संकेतस्थळ निरीक्षण योजना

संकेतस्थळाच्या गुणवत्तेचे व सुसंगतीचे परीक्षण करण्यासाठी नियमितपणे निरीक्षण केले जाते. खालील बाबींवर विशेष लक्ष दिले जाते:

- **कार्यक्षमता:** विविध नेटवर्क कनेक्शन व उपकरणांवर साइट लवकर लोड होईल याची काळजी घेतली जाते.
- **कार्यप्रदर्शन:** सर्व मॉड्युल्स व संवादात्मक घटक (जसे अभिप्राय फॉर्म) नीट कार्यरत असल्याची खात्री केली जाते.
- **तुटलेले दुवे:** संपूर्ण पोर्टल तपासून तुटलेले दुवे अथवा त्रुटी दूर केल्या जातात.
- **वाहतूक विश्लेषण:** संकेतस्थळावरील अभ्यागतांचे वापर पद्धती तपासल्या जातात.
- **अभिप्राय:** अभ्यागतांनी दिलेल्या सूचनांनुसार बदल व सुधारणा केली जाते.

आकस्मिक व्यवस्थापन योजना (Contingency Management Plan)

आकस्मिक योजना तयार करणे हे सज्जता सुनिश्चित करण्यासाठी आणि विकृतीकरण (defacement) किंवा नैसर्गिक आपत्तींचा परिणाम कमी करण्यासाठी अत्यंत महत्वाचे आहे. आकस्मिक योजना तयार करताना आम्ही खालील बाबी विचारात घेतल्या आहेत:

१. जोखीम मूल्यांकन (Risk Assessment):

आमच्या संस्थेसमोर उद्भवू शकणाऱ्या संभाव्य जोखीम व कमकुवत बाजूंची आम्ही ओळख केली आहे, जसे की मालमत्तेचे विकृतीकरण किंवा पूर, भूकंप, वादळ, आगीसारख्या नैसर्गिक आपत्ती. प्रत्येक जोखीम उद्भवण्याची शक्यता आणि संभाव्य परिणाम यांचे आम्ही मूल्यांकन केले आहे.

२. आपत्कालीन प्रतिसाद पथक (Emergency Response Team):

आम्ही विविध विभागातील प्रमुख व्यक्तींना सामावून घेणारे आपत्कालीन प्रतिसाद पथक स्थापन केले आहे. आपत्कालीन परिस्थितीत त्यांची भूमिका व जबाबदाऱ्या निश्चित केल्या आहेत. तसेच संपूर्ण प्रतिसादाचे समन्वयन करण्यासाठी आम्ही एक टीम लीडर नियुक्त केला आहे.

३. संवाद योजना (Communication Plan):

आम्ही कर्मचाऱ्यांशी, भागधारकांशी व जनतेशी परिणामकारक संवाद साधता यावा यासाठी स्पष्ट संवाद योजना तयार केली आहे. या योजनेमध्ये ईमेल, मजकूर संदेश, सामाजिक माध्यमे व निश्चित संपर्क बिंदू यांसारख्या विविध संवाद साधनांचा समावेश आहे.

४. डेटा बॅकअप व पुनर्प्राप्ती (Data Backup and Recovery):

आम्ही नियमितपणे महत्त्वपूर्ण डेटाचा बॅकअप घेऊन तो क्लाउडमध्ये सुरक्षितरीत्या साठवतो. विकृतीकरण किंवा डेटा गमावल्यास आवश्यक प्रणाली व डेटाची पुनर्प्राप्ती सुनिश्चित करण्यासाठी आम्ही डेटा पुनर्प्राप्ती योजना आखली आहे.

५. भौतिक सुरक्षा उपाय (Physical Security Measures):

आमच्या संस्थेची संपत्ती सुरक्षित ठेवण्यासाठी आम्ही निरीक्षण प्रणाली (CCTV), प्रवेश नियंत्रण, अलार्म इत्यादी सुरक्षा उपाय अंमलात आणले आहेत. तसेच विध्वंसक कृत्ये किंवा विकृतीकरणापासून संरक्षणाचे उपायही विचारात घेतले आहेत.

६. प्रशिक्षण व सराव (Training and Drills):

आम्ही नियमितपणे प्रशिक्षण सत्रे व आपत्कालीन सराव आयोजित करतो, ज्यामुळे कर्मचाऱ्यांना आपत्कालीन प्रक्रियेबद्दल व त्यांच्या भूमिकेबद्दल माहिती मिळते. या सरावामुळे सर्वांना आकस्मिक योजनेची ओळख होते आणि ते सज्ज राहतात.

७. पुनर्प्राप्ती व पुनर्संचयितीकरण (Recovery and Restoration):

घटनानंतर पुनर्प्राप्ती व सामान्य कार्यपद्धती पुन्हा सुरू करण्यासाठी आम्ही धोरणे विकसित केली आहेत. यामध्ये नुकसानाचे मूल्यांकन, दुरुस्ती, आवश्यक सेवा पुन्हा सुरू करणे आणि प्रभावित कर्मचाऱ्यांना मदत करणे या प्राधान्यक्रमांचा समावेश आहे.

८. नियमित पुनरावलोकन व अद्ययावत करणे (Regular Plan Review and Updates):

आम्ही आमच्या आकस्मिक योजनेचे सतत पुनरावलोकन व अद्ययावत करतो. सराव, प्रत्यक्ष घटना किंवा संस्थेच्या रचनेतील बदलांमधून शिकलेल्या धड्यांचा समावेश करतो. त्यामुळे योजना सद्यस्थितीनुसार उपयुक्त व प्रभावी राहते.

व्यवसाय सातत्य योजना (Business Continuity Plan - BCP)

संस्थेसाठी व्यवसाय सातत्य योजना (BCP) तयार करताना कार्यपद्धती, महत्त्वाच्या प्रक्रिया आणि संभाव्य जोखमींची सखोल समज असणे आवश्यक आहे. अशा योजनेसाठी आम्ही खालील महत्त्वाचे टप्पे विचारात घेतले आहेत:

१. व्यवसाय परिणाम विश्लेषण (Business Impact Analysis - BIA):

आम्ही संस्थेच्या महत्त्वपूर्ण कार्ये, प्रक्रिया आणि परावलंबन यांचे सविस्तर मूल्यांकन केले आहे. संभाव्य जोखीमांची ओळख करून घेतली आहे आणि कार्यात व्यत्यय आल्यास आर्थिक नुकसान, प्रतिष्ठेवर परिणाम व ग्राहक असमाधान यांसारखे परिणाम निश्चित केले आहेत.

२. जोखीम मूल्यांकन (Risk Assessment):

आम्ही आमच्या संस्थेशी संबंधित जोखमींचे मूल्यांकन केले आहे, जसे की नैसर्गिक आपत्ती, सायबर धोके, पुरवठा साखळीतील व्यत्यय आणि इतर संभाव्य संकटे. या जोखीमांची शक्यता व व्यवसायावर होणारा परिणाम लक्षात घेऊन त्यांना प्राधान्यक्रम दिला आहे.

३. पुनर्प्राप्ती उद्दिष्टे (Recovery Objectives):

प्रत्येक महत्त्वाच्या प्रक्रियेसाठी आम्ही पुनर्प्राप्ती वेळ उद्दिष्ट (RTO) आणि पुनर्प्राप्ती बिंदू उद्दिष्ट (RPO) निश्चित केले आहेत. RTO म्हणजे प्रक्रियेसाठी स्वीकार्य ठप्पावस्था कालावधी, तर RPO म्हणजे स्वीकार्य डेटा नुकसानाची कमाल मर्यादा.

४. सातत्य धोरणे (Continuity Strategies):

व्यत्यांचा परिणाम कमी करण्यासाठी आणि कार्य सातत्य सुनिश्चित करण्यासाठी आम्ही विविध धोरणे विकसित केली आहेत. यात दुहेरी प्रणाली (redundant systems), पर्यायी पुरवठादार, बॅकअप सुविधा, क्लाउड-आधारित सेवा आणि दूरस्थ कार्य (remote work) यांचा समावेश आहे. प्रत्येक धोरणाची किंमत, व्यवहार्यता आणि प्रभावीपणा तपासला आहे.

५. आपत्कालीन प्रतिसाद योजना (Emergency Response Plan):

आम्ही एक आपत्कालीन प्रतिसाद पथक तयार केले आहे आणि आपत्तीच्या वेळी त्यांच्या भूमिका व जबाबदाऱ्या निश्चित केल्या आहेत. संकटाच्या वेळी अंतर्गत व बाह्य संवाद सुरळीत राहावा यासाठी स्पष्ट संवाद योजना तयार केली आहे. प्राथमिक व पर्यायी संवाद साधनांची ओळख करून दिली आहे.

६. डेटा बॅकअप व पुनर्प्राप्ती (Data Backup and Recovery):

आम्ही एक मजबूत डेटा बॅकअप व पुनर्प्राप्ती प्रणाली अंमलात आणली आहे. नियमितपणे महत्त्वपूर्ण डेटाचा बॅकअप घेतो आणि तो सुरक्षित स्थळी किंवा क्लाउड-आधारित सोल्यूशन्समध्ये साठवतो. डेटा पुनर्प्राप्ती प्रक्रियेची चाचणी घेऊन डेटाची अखंडता व उपलब्धता सुनिश्चित करतो.

७. घटना व्यवस्थापन (Incident Management):

घटना ओळखणे, अहवाल देणे व तात्काळ प्रतिसाद देण्यासाठी आम्ही प्रक्रिया विकसित केल्या आहेत. आपत्तीच्या काळात कार्यवाढ (escalation), निर्णयप्रक्रिया आणि समन्वयासाठी प्रोटोकॉल निश्चित केले आहेत. कर्मचाऱ्यांना घटना व्यवस्थापन प्रक्रियेबद्दल व त्यांच्या भूमिकेबद्दल प्रशिक्षण दिले आहे.

८. चाचणी व प्रशिक्षण (Testing and Training):

आम्ही नियमितपणे BCP सराव व चाचण्या घेतो, ज्याद्वारे योजनेची कार्यक्षमता तपासली जाते. आढळलेल्या उणिवा दूर करून योजना अद्ययावत केली जाते. आपत्कालीन परिस्थितीत कर्मचाऱ्यांची भूमिका व जबाबदाऱ्या समजण्यासाठी प्रशिक्षण दिले जाते.

९. योजनेचे देखभाल व पुनरावलोकन (Plan Maintenance and Review):

संस्था विकसित होत असताना किंवा नवे धोके उद्भवत असताना आम्ही व्यवसाय सातत्य योजना सतत पुनरावलोकन व अद्ययावत करतो. संपर्क यादी, आपत्कालीन प्रक्रिया व पुनर्प्राप्ती धोरणे अद्ययावत ठेवतो. तसेच योजनेचे पालन सुनिश्चित करण्यासाठी नियमित लेखापरीक्षण (audit) करतो.

व्यवसाय सातत्य योजनेत संकेतस्थळ विकृतीकरण (Defacement of the Website)

संकेतस्थळ विकृतीकरणाची घटना हाताळणे हे व्यवसाय सातत्य योजनेचा महत्त्वपूर्ण भाग आहे. यामध्ये संकेतस्थळाची कार्यक्षमता, प्रतिष्ठा आणि सुरक्षा पुनर्संचयित करण्यासाठी ठोस उपायांचा समावेश होतो. त्यासाठी आम्ही खालील पद्धत अवलंबली आहे:

१. शोध आणि प्रतिसाद (Detection and Response):

- आमच्या संकेतस्थळावर नियमित देखरेख ठेवली जाते जेणेकरून विकृतीकरणाची कोणतीही लक्षणे ओळखता येतील.

- प्रारंभिक शोधासाठी Intrusion Detection Systems आणि Web Application Firewalls यांसारखी सुरक्षा साधने लागू केली आहेत.
- विकृतीकरण आढळल्याबरोबर आम्ही Incident Response Plan सुरू करतो आणि नियुक्त प्रतिसाद पथकाला कळवतो.
- विकृतीकरणाचा व्याप्ती तपासून पुरावा गोळा करतो (उदा. स्क्रीनशॉट किंवा संबंधित पृष्ठांचे दस्तऐवजीकरण).

२. वेगळे करणे व तपासणी (Isolate and Investigate):

- प्रभावित संकेतस्थळ तात्काळ वेगळे करून अधिक नुकसान किंवा शिरकाव रोखला जातो.
- सखोल तपासणी करून विकृतीकरणाची कारणे आणि प्रमाण शोधले जाते. संकेतस्थळातील संभाव्य त्रुटी व कमकुवत बाजूंची ओळख केली जाते.

३. बॅकअपमधून पुनर्संचयितीकरण (Restore from Backup):

- विकृतीकरण होण्यापूर्वीचा ज्ञात स्वच्छ बॅकअप वापरून संकेतस्थळ पुनर्संचयित केले जाते.
- बॅकअप सुरक्षित आहे आणि त्यामध्ये कोणताही दूषित कोड किंवा त्रुटी नाहीत याची खात्री केली जाते.
- पुनर्संचयित संकेतस्थळाची कार्यक्षमता व्यवस्थित तपासली जाते.

४. त्रुटीनिवारण व सुरक्षा (Patch and Secure):

- विकृतीकरणाला कारणीभूत ठरलेल्या कमकुवत बाजू व त्रुटी दूर केल्या जातात.
- संकेतस्थळाचे सॉफ्टवेअर, प्लगिन्स, थीम्स व इतर घटक अद्ययावत केले जातात.
- मजबूत प्रमाणीकरण यंत्रणा, नियमित सुरक्षा लेखापरीक्षण (audits) आणि Web Application Firewalls लागू करून भविष्यातील विकृतीकरण प्रयत्नांना आळा घालण्यात येतो.

५. पुनरावलोकन व चाचणी (Review and Test):

- घटनेचे सखोल पुनरावलोकन करून घेतलेल्या धड्यांची नोंद केली जाते. प्रतिसाद आणि पुनर्प्राप्ती प्रक्रियेची कार्यक्षमता तपासली जाते.

- उरलेल्या सुरक्षा त्रुटी ओळखण्यासाठी व दुरुस्तीसाठी Penetration Testing व Vulnerability Assessments केले जातात.
- संकेतस्थळाची सुरक्षा व कार्यक्षमता नियमितपणे तपासली जाते जेणेकरून भविष्यातील धोके टाळता येतील.

६. संवाद व प्रतिष्ठा व्यवस्थापन (Communication and Reputation Management):

- भागधारक, ग्राहक आणि वापरकर्त्यांना घटनेची माहिती, केलेली पावले आणि भविष्यातील प्रतिबंधात्मक उपाय याविषयी कळवण्यासाठी संवाद योजना तयार केली आहे.
- भागधारकांनी उपस्थित केलेल्या प्रश्नांना व शंका स्पष्ट करण्यासाठी आम्ही पारदर्शक व सक्रिय पद्धतीने संवाद साधतो.
- संकेतस्थळाच्या प्रतिष्ठेवर होणाऱ्या नकारात्मक परिणामावर देखरेख ठेवून त्याला त्वरित प्रतिसाद दिला जातो.
- विश्वास व आत्मविश्वास पुनर्संचयित करण्यासाठी आवश्यक तेवढ्या जनसंपर्क कृती (PR activities) केल्या जातात.

आपत्ती पुनर्प्राप्ती (Disaster Recovery - DR) अंतर्गत डेटा Corruption निराकरण

DR साइटवरील डेटा Corruption हाताळणे म्हणजे डेटा अखंडता (integrity) पुनर्संचयित करणे आणि व्यवसाय सातत्य सुनिश्चित करण्यासाठी एक पद्धतशीर दृष्टिकोन अवलंबणे होय. डेटा भ्रष्टाचार सोडवण्यासाठी आम्ही खालील सर्वसाधारण पावले विचारात घेतली आहेत:

१. भ्रष्ट डेटा ओळखणे आणि वेगळे करणे (Identify and Isolate Corrupted Data):

- डेटा भ्रष्टाचाराचा व्याप्ती आणि प्रमाण निश्चित केले जाते. कोणती फाइल्स, डेटाबेस किंवा प्रणाली प्रभावित झाली आहे ते शोधले जाते.
- भ्रष्ट डेटा वेगळा करून आणखी नुकसान किंवा प्रसार होऊ नये याची खबरदारी घेतली जाते. यामध्ये प्रभावित प्रणाली नेटवर्कपासून वेगळ्या करणे किंवा भ्रष्ट फाइल्सवरील प्रवेश अक्षम करणे यांचा समावेश असतो.

२. मूळ कारण शोधणे (Determine the Source and Cause):

- डेटा भ्रष्टाचाराची कारणे तपासली जातात. हे हार्डवेअर बिघाड, सॉफ्टवेअरमधील दोष, मानवी चूक, मालवेअर किंवा इतर घटकांमुळे होऊ शकते.

- भ्रष्टाचार प्राथमिक साइटवर झाला की DR साइटवर प्रतिकृतीकरण (replication) प्रक्रियेदरम्यान झाला हे निश्चित केले जाते. यामुळे योग्य निराकरण उपाय ठरवणे सोपे जाते.

३. बॅकअपमधून पुनर्संचयित करणे (Restore from Backup):

- प्रभावित डेटाचा स्वच्छ बॅकअप वापरून पुनर्संचयितीकरण प्रक्रिया सुरू केली जाते. बॅकअप भ्रष्टाचाराने प्रभावित नसल्याची खात्री केली जाते.
- बॅकअपची अखंडता पडताळून पाहिली जाते आणि पुनर्संचयित डेटा अपेक्षित स्थितीशी जुळत असल्याची खात्री केली जाते.

४. डेटा समक्रमण आणि ताळमेळ (Data Synchronization and Reconciliation):

- जर डेटा भ्रष्टाचार DR साइटवर प्रतिकृतीकरणाच्या वेळी झाला असेल, तर समक्रमण प्रक्रिया सुरू करून डेटा ताळमेळ साधला जातो.
- वापरल्या जाणाऱ्या प्रतिकृतीकरण पद्धती व तंत्रज्ञानानुसार दस्तऐवजांचा संदर्भ घेतला जातो किंवा विक्रेत्याशी (vendor) संपर्क साधून योग्य मार्गदर्शन घेतले जाते.

५. डेटा दुरुस्ती व पुनर्प्राप्ती (Data Repair and Recovery):

- ज्या ठिकाणी भ्रष्ट डेटा बॅकअप किंवा समक्रमणातून पुनर्संचयित होऊ शकत नाही, तिथे डेटा दुरुस्ती तंत्रांचा विचार केला जातो.
- यामध्ये विशेष साधने वापरणे किंवा डेटा पुनर्प्राप्ती तज्ज्ञांची मदत घेणे समाविष्ट असते, ज्यामुळे भ्रष्ट डेटा वाचवून दुरुस्त करता येतो.

६. डेटा पडताळणी व चाचणी (Data Validation and Testing):

- डेटा पुनर्संचयितीकरण व दुरुस्ती प्रक्रिया पूर्ण झाल्यावर पुनर्प्राप्त केलेल्या डेटाची अखंडता व अचूकता पडताळली जाते.
- डेटा वापरण्यास योग्य आहे आणि भ्रष्टाचारमुक्त आहे याची खात्री करण्यासाठी सखोल चाचणी व सत्यापन केले जाते.

७. प्रणाली व प्रक्रिया सुधारणा (System and Process Improvements):

- डेटा भ्रष्टाचाराच्या घटनेचे मूळ कारण विश्लेषित केले जाते व प्रणाली किंवा प्रक्रियेतील कमकुवत बाजू शोधल्या जातात.
- भविष्यातील भ्रष्टाचार टाळण्यासाठी योग्य उपाययोजना केल्या जातात. यामध्ये हार्डवेअर सुधारणा, सॉफ्टवेअर अद्यतने, सुधारित बॅकअप व प्रतिकृतीकरण प्रक्रिया किंवा अधिक प्रभावी डेटा पडताळणी तपासण्या यांचा समावेश आहे.

८. दस्तऐवजीकरण व संवाद (Documentation and Communication):

- डेटा भ्रष्टाचार निराकरणासाठी केलेल्या सर्व पायऱ्यांचे दस्तऐवजीकरण केले जाते, ज्यामध्ये मूळ कारण विश्लेषण व डेटा पुनर्प्राप्तीसाठी केलेल्या कृतींचा समावेश असतो.
- IT टीम्स, व्यवस्थापन व प्रभावित वापरकर्त्यांना घटनेबद्दल, घेतलेल्या उपाययोजनांबद्दल व अंमलात आणलेल्या प्रतिबंधात्मक उपायांबद्दल माहिती दिली जाते.

नैसर्गिक आपत्ती – DR (Disaster Recovery) आणि DC (Data Centre) यांच्या संदर्भात

DR (आपत्ती पुनर्प्राप्ती) आणि DC (डेटा सेंटर) हे एकमेकांशी घनिष्ठपणे संबंधित संकल्पना आहेत आणि नैसर्गिक आपत्तीमुळे व्यवसायाच्या कामकाजावर होणारा परिणाम कमी करण्यासाठी दोन्ही अत्यंत महत्त्वाची भूमिका बजावतात. खाली त्यांचा परस्पर संबंध कसा आहे याचा आढावा दिला आहे:

आपत्ती पुनर्प्राप्ती (Disaster Recovery – DR):

- DR म्हणजे धोरणे, प्रक्रिया आणि कार्यपद्धती ज्यांचा उपयोग नैसर्गिक आपत्ती किंवा कोणत्याही मोठ्या व्यत्ययामुळे विस्कळीत झालेल्या महत्त्वाच्या व्यवसाय कार्ये व IT प्रणाली पुनर्संचयित करण्यासाठी केला जातो.
- DR योजना ही आपत्तीच्या परिस्थितीत downtime कमी करण्यासाठी, डेटा पुनर्प्राप्त करण्यासाठी आणि व्यवसाय पुन्हा सुरू करण्यासाठी घ्यावयाच्या पायऱ्या स्पष्ट करते.
- DR सहसा ऑफ-साइट ठिकाणी redundant प्रणाली, डेटा बॅकअप आणि पर्यायी इन्फ्रास्ट्रक्चर ठेवून व्यवसाय सातत्य (Business Continuity) सुनिश्चित करते.

डेटा सेंटर (Data Centre – DC):

- डेटा सेंटर हे संगणक प्रणाली, सर्व्हर्स, नेटवर्क उपकरणे व डेटा साठवण संसाधने ठेवण्यासाठीची भौतिक सुविधा आहे.
- डेटा सेंटर हे अत्यावश्यक IT इन्फ्रास्ट्रक्चर सुरक्षित व नियंत्रित वातावरणात ठेवण्यासाठी डिझाइन केलेले असते.
- यामध्ये redundant वीजपुरवठा, शीतकरण प्रणाली (Cooling Systems), अग्निशमन व्यवस्था (Fire Suppression Measures), आणि भौतिक सुरक्षा उपाय असतात, ज्यामुळे उपकरणांचे रक्षण होते व अखंडित कामकाज शक्य होते.

नैसर्गिक आपत्तींच्या संदर्भात DR आणि DC यांचे परस्पर संबंध:

- नैसर्गिक आपत्तीमुळे (जसे पूर, भूकंप, वादळ, आग इ.) डेटा सेंटर प्रभावित झाले, तर DR प्रणाली आणि बॅकअप साइट्समुळे व्यवसाय सातत्य राखता येते.
- डेटा सेंटरमध्ये असलेल्या redundant सुविधा आणि सुरक्षा उपाय आपत्तीचा तात्काळ परिणाम कमी करतात, परंतु मोठ्या आपत्तीत DR योजना सक्रिय करून कामकाज ऑफ-साइट स्थानावरून सुरू केले जाते.
- DR आणि DC हे एकमेकांचे पूरक असून, दोन्ही एकत्रितपणे संस्थेच्या IT इन्फ्रास्ट्रक्चरचे संरक्षण आणि सातत्य राखतात.

संकेतस्थळ सुरक्षा धोरण (Website Security Policy)

म्हाडा सुरक्षित सर्व्हर्स आणि योग्य सुरक्षा उपायांचा अवलंब करते. यामध्ये नेटवर्क ट्रॅफिकचे निरीक्षण करून डेटाची अखंडता जपली जाते आणि अनधिकृत प्रवेश रोखला जातो.

माहिती अपलोड करणे, बदल करणे, सुरक्षा उपाय निष्फळ करणे किंवा संकेतस्थळास हानी पोहोचवण्याचे कोणतेही प्रयत्न कडकपणे निषिद्ध आहेत. असे प्रयत्न झाल्यास संबंधित IT आणि सायबर कायद्यांनुसार कायदेशीर कारवाई करण्यात येईल.

सुरक्षा भंग (breach) झाल्यास म्हाडा तपास आणि कारवाईसाठी संबंधित माहिती कायदा अंमलबजावणी संस्थांसोबत (law enforcement authorities) सामायिक करू शकते.

वेब माहिती व्यवस्थापक

नाव: संदीप बोदले, आयसीटी अधिकारी

संपर्क: ०२२-६६४०५०००