Approved By	Controlled By
HOD(C&IT)	CISO

Document Name	**Risk register**
Document Version	**1.0**
Document ID	**ISMS/DOC/Register/01**
Security Classification	**Confidential**
Review Frequency	**Annually**
Date	**19.05.2025**

Document Change Record

Version History:

Sl. NO.	Version	Issue Date	Prepared By	Reviewed By	Approved By	Change Description
1.	1.0	19.05.2025	Shweta Roy Sr. Mgr (C&IT) 19.05.2025	A K Choudhry CISO, GM(C&IT) 19.05.2025	Rajan Kumar CGM (C&IT) 19.05.2025	Initial Release

Distribution List:

- C&IT Department
- ISMS Security Forum

Notes:

- This is a controlled document under ISO 27001 ISMS. Unauthorized changes are prohibited.
- Ensure the most recent version is used at all times.
- All changes must be recorded in the Document Change Record section.

1. Introduction

This Risk Register documents identified information security risks within the scope of Bokaro Steel Plant's Information Security Management System (ISMS), covering the information assets, IT infrastructure of the Computer & Information Technology Department and its operations in accordance with the Statement of Applicability.

2. Risk Register

Risk ID	Risk Description	Asset(s) Affected	Threat Source	Vulnerability	Asset Value (1-5)	Threat Likelihood (1-5)	Vulnerability Level (1-5)	Impact (1-5)	Inherent Risk Score	Existing Controls	Control Effectiveness (0.1-0.9)	Residual Risk Score	Risk Level	Risk Owner	Risk Treatment Option	Risk Treatment Plan	Status	Next Review Date
R-001	Unauthorized access to sensitive customer data	Customer database	External hackers	Weak authentication mechanisms	5	4	4	5	80	1. Password policy 2. Firewall 3. Access logs4.SSL certificates	0.5	40	Medium	Database Administrator	Mitigate	1. Implement MFA	In Progress	December, 2025
R-	Data loss due to	File servers,	System failure,	Inconsistent	5	3	4	5	60	1.Daily backups 2. Disk Backup 3. Test restore	0.5	30	Me	Back up	Mitigate			

002	inadequate backup procedures	application servers	human error	backup processes						procedures semi-annually			dium	Administrator				
R-003	Malware infection	Workstations, servers, PCs	Email attachments, malicious websites	Outdated antivirus, user behavior	4	4	3	4	48	1. Antivirus software 2. Email filtering	0.5	24	Low	IT Security Team	Mitigate	1. Deploy EDR solution 2. Enhance user awareness training 3. Implement application whitelisting	In Progress	December, 2025
R-004	Network intrusion	Network infrastructure	External attackers	Firewall misconfigurations	5	3	3	5	45	1. Firewall 2. Network segmentation 3. IDS 4.Antivirus 5. Domain Control	0.5	22.5	Low	Network Administrator	Mitigate	1. Conduct firewall rule review 2. Implement regular vulnerability scanning 3. Deploy EDR solution	Planned	December, 2025
R-005	Service disruption due to DDoS attack	Internet Services	Hacktivists, competitors	Insufficient DDoS protection	4	3	4	4	48	1. Basic firewall 2. Rate limiting 3. Redundant Firewall in place	0.7	33.6	Medium	Network Administrator	Mitigate			
R-	Data breach	Customer	Disgruntled	Excessive	5	2	4	5	40	1. Access controls 2. HR policies 3. Least privilege	0.7	28	Me	HR, IT	Mitigate	1. Regular access reviews 2. Employee		

006	due to insider threat	database, intellectual property	employees	user privileges						model implemented			dium	Security		monitoring		
R-007	Physical security breach	Server room, network equipment	Unauthorized personnel	Inadequate physical access controls	5	2	3	4	30	1. Lock and key 2. CCTV 3.Biometric entry in server rooms 3. Access card system implemented 4. Visitor management procedures in place 5. CCTV coverage	0.5	15	Low	Facilities Manager	Mitigate			
R-008	System unavailability due to patching failures	Critical business applications	System administrators	Inadequate change management	4	3	3	4	36	1. Change management process 2. Test environment 3. Rollback capabilities implemented	0.5	18	Low	Change Manager	Mitigate			
R-009	Data corruption due to software defects	Business applications	Software bugs	Insufficient testing	4	3	3	4	36	1. Development standards 2. User acceptance testing	0.5	18	Low	Development Manager	Mitigate			
R	Ransom	All	Phishin	User	5	4	4	5	80	1. Antivirus 2. Email filtering	0.5	40	M	IT	Miti	1. Implement	In	De

-010	ware attack	systems	g emails, drive-by downloads	behavior, security gaps						3. Backups			edium	Security Team	gate	application whitelisting 2. Enhanced user training 3. Network segmentation 4. Offline backups	Progress	cember, 2025
R-011	Vendor security breach	Third-party systems with access	External attackers	Inadequate vendor controls	4	3	4	4	48	1. Vendor assessment 2. Contract clauses - NDA	0.7	33.6	Medium	Procurement, IT Security	Mitigate			
R-012	Privileged account compromise	Domain controllers, critical servers	Targeted attack	Weak privileged account security	5	3	4	5	60	1. Password policy 2. Access control	0.7	42	Medium	IT Security Team	Mitigate			
R-013	Business interruption due to power failure	Server room, network equipment	Power grid failure	Dual power source	5	2	3	5	30	1. UPS systems 2. Backup generators	0.5	15	Low	Facilities Manager	Mitigate & Accept	1. Test generator monthly	Planned	
R	Web	Custom	Extern	Applic	5	4	3	5	60	1. Web application firewall 2.	0.5	30	M	Appl	Miti	1. Developer		

-014	application compromise	er-facing web applications	al attackers	ation vulnerabilities						Secure coding practices 3. Implement regular VAPT scanning			edium	ication Security Team	gate	security training		
R-015	Social engineering attack	All users with system access	Targeted phishing	User awareness gaps	4	4	4	4	64	1. Basic awareness training 2. Email filtering	0.7	44.8	Medium	IT Security Team	Mitigate	1. Regular awareness training 2. Security culture program	In Progress	Every month
R-016	Database injection attack	Application database	External attackers	Poor input validation	5	3	4	5	60	1. Basic input filtering 2. Database permissions 3. Parameterized queries implemented 4. Database monitoring	0.6	24	Low	Database Administrator	Mitigate			
R-017	Certificate expiration	SSL/TLS certificates	Certificate authority	Poor certificate management	3	4	2	3	24	1. Certificate monitoring 2. Renewal reminders 3. Certificate inventory 4. Early warning system	0.8	19.2	Low	IT Operations	Mitigate		Planned	
R-	DNS poisonin	DNS infrastr	External	Unsecured	4	2	3	4	24	1. DNS filtering 2. Monitoring 3.Multiple DNS in place(4	0.7	16.8	Lo	Networ	Mitigate	1. Implement DNS security extensions	Pla	Dece

018	g attack	ucture	attackers	DNS configuration						nos).			w	k Administrator		2. Secondary DNS providers 3. DNS monitoring tools	nned	mber, 2025
R-019	Wireless network compromise	WiFi infrastructure	External attackers	Weak WiFi security	3	3	4	3	36	1. WPA2 encryption 2. Network isolation 3. Guest network segregation	0.6	14.4	Low	Network Administrator	Mitigate	1. Implement network access control	In Place	
R-020	Email compromise	Email servers	Phishing, credential theft	Weak email security	4	4	3	4	48	1. Spam filtering 2. Basic authentication 3. DMARC/SPF/DKIM in NIC email	0.6	19.2	Low	IT Security Team	Transfer & Mitigate			
R-021	Remote access compromise	VPN infrastructure	External attackers	Weak VPN security	4	3	4	4	48	1. VPN access controls 2. Authentication 3. Zero-trust VPN Implemented 4. Multi-factor authentication	0.6	19.2	Low	Network Administrator	Mitigate	1. Session monitoring		
R-0	Business email compro	Executive email	Social engineering	Weak email contro	4	3	4	5	60	1. Email filtering 2. User awareness	0.6	24	Low	IT Security	Transfer			

22	mise	accounts		ls										Team	& Mitigate			

3. Risk Assessment Summary

3.1 Risk Level Distribution

Risk Level	Count	Percentage
Critical	0	0%
High	0	0%
Medium	8	36.4%
Low	14	63.6%
Very Low	0	0%
Total	**20**	**100%**

3.2 Risk Treatment Summary

Treatment Option	Count	Percentage
Mitigate	20	90.9.%
Transfer & Mitigate	2	9.09%

Mitigate & Accept	0	0%
Accept	0	0%
Avoid	0	0%
Total	**22**	**100%**

Note: This Risk Register is a living document that should be reviewed and updated regularly according to the organization's Risk Management Policy and Risk Assessment Methodology.

Policy Review: This Risk Register will be reviewed annually or after significant changes to ensure continued effectiveness and alignment with ISO 27001:2022 standards.

END OF DOCUMENT