KRBL Limited

World's Largest Rice Millers & Basmati Rice Exporters

IT Cyber Security Policy

Version 1.0

Authorized Signatory		
Name	Date	Signature
	01-05-2023	

26/04/2023

S.No.	Type of Information	Document Data
1	Document Title	Cyber Security Policy
2	Document Code	KRBL/IS/POL/CSP
3	**Date of Release**	30.05.2023
5	Document Revision No.	1.0
6	Document Reviewer	
7	Document Author(s)	GM IT
8	Document Owner	VP-IT / CIO / IT Head / GM IT

B. Document Review and Approval History

Date	Version	Amended by	Reviewer/Approver	Remarks	RFC#

Disclaimer

26/04/2023

Contents

26/04/2023

1.0 Introduction

To combat growing cyber threats and to enhance resilience of the KRBL Limited (hereinafter referred as "KRBL") to address cyber risks, this Cyber Security Policy (hereafter referred to as CSP) is developed. CSP is a structured approach to set out the management strategy to address cyber security concerns and the responsibilities of all personnel to prevent breaches of cyber security, and protect KRBL's business.

2.0 Objective

The objectives of Cyber Security policy are:

- To provide support and direction on different aspects of cyber security
- To ensure compliance of legal, regulatory, and contractual requirements
- To create and maintain a security-conscious culture in KRBL

3.0 Scope

This policy shall be applicable to all employees of KRBL, off-roles employees and third party contractors utilizing KRBL IT assets, IT operations and all KRBL office locations. Any violation to Cyber Security Policy may lead to disciplinary/ legal action.
This document shall be approved by the CIO/ VP-IT/ IT Head.

4.0 Review of Cyber Security Policy (CSP)

- The CSP should be reviewed at least once in 2 years or whenever significant changes occur in relevant ecosystem.
- Chief Information Officer (CIO) is the owner of the CSP document. The overall owner of the cyber security initiative within the KRBL is CIO/ VP-IT/ IT Head.

5.0 Cyber Security Governance

- Cyber Security Governance Structure consists of the CIO/ VP-IT, IT Head and CISO, Deputy IT Head, System Admin.
- CIO/ VP-IT / IT-Head shall also be part of the overall Cyber Security Governance Structure.
- These personnel are responsible for development, implementation, operation, maintenance and continual improvement of Cyber Security.

6.0 Information Sharing & External Relations

- Contacts with law enforcement authorities, fire department, emergency services shall be maintained by CIO office. CIO shall put in place information sharing arrangements with CERT-In
- Information Asset Owner shall ensure compliance to each of the Laws and Acts relevant to its operations. These shall include but not limited to the Information Technology (IT) Act, Intellectual Property Rights (IPR), etc.

26/04/2023

7.0 Secure IT Architecture

- Following aspects shall be integral part of KRBL's IT Architecture:
- KRBL's all critical applications including outsourced shall be hosted in Layer-3 / proper secured environment data centre.

Application Usage	Example	RPO	RTO	Backup Server	DR Site
Business Application (ERP)	Treasury	30 Minutes	30 Minutes	Y	N
Internal Collaboration	Mail	24 Hours	4 Hours	Y	Y
HRMS		30 Minutes	30 Minutes	Y	Y

- IDS, IPS, Firewalls, Internet Gateway, Mail Gateway, DDOS protector, Application Delivery Controllers, DNS servers, Routers & Switches etc. shall have secure configuration and shall be part of continuous surveillance.
- KRBL shall deploy Antivirus, Anti-malware solution to cover all computing devices, including mobile devices/mobile phones. Devices which shall be out of this framework needs to be identified and recorded in ITSC meeting with reasons, probable risks and compensating controls.
- All new applications, modules shall be subjected to IS Audit and User Acceptance Test (UAT) and cleared by CIO before launch. In case of business requirement and meeting minimum level of safeguards, CIO is empowered to permit launch for a limited period (not more than 6 months) after completion of User Acceptance Test.
- Baseline Cyber Security and Resilience Requirement shall be implemented in a phased manner. Implementation status to be reported in quarterly ITSC meetings.

8.0 Continuous Surveillance

- Vulnerability Assessment (VA), Security Device Configuration, Penetration Testing (PT), Application Security Testing (APPSEC) & Process review shall be performed at least on annual basis for all information system processes and associated production setup. The Asset Owners shall evaluate such vulnerabilities and appropriate measures shall be taken to address the associated risk.
- To anticipate the unknown Cyber-attacks and evolving threat landscape, the KRBL has set up a NOC (network Operations Centre). NOC shall ensure continuous surveillance through event logs, alerts and advisories received through external relationships. NOC operations shall be headed by officer not below the rank of Senior Manager. NOC Manager shall keep CIO office updated on the abnormal events detected on real-time basis.
- NOC manager shall develop a standard operating procedure (SOP) duly approved by the Steering Committee, for detection of infrastructure logs with any malicious or suspicious events.

26/09/2023

9.0 Inventory Management of IT Assets

- CIO office shall maintain all Information System Process (updated on quarterly basis) with OS, DB versions, Asset/Process Ownership, Custodians, Criticality and Audit Frequency.
- Complete inventory of IT assets shall be maintained for each process by Process Asset Owners, with hardware Software, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) responsible for the asset to be maintained.

10.0 Maintenance of Information Assets

- Asset owners shall issue suitable guidelines through internal communications for acceptable usage of Information Assets.
- IT Head shall ensure enterprise architecture is defined, developed and periodically reviewed so that manual and administrative controls can be converted into automated one especially end-point control, license compliance, patch management, access control, contract management and performance management. Absence of automation should not result in absence of controls even through administrative orders and manual efforts.
- Every Information Asset user shall be made aware of potential hazard of non-compliance of guidelines through continuous awareness programme using Intranet, SMS, Emails, Trainings or any other media. User shall be made aware that non-compliance shall result in suitable disciplinary proceedings on detection by KRBL's HR department.
-

11.0 Removable Media handling

- Removable Media is not permitted to be connected on KRBL's networked computers. In case of business requirement, specific written permission to be obtained from CIO / IT-Head
- IT department shall implement system related controls wherein USB ports shall be disabled and if enabled after change request process, controls through Data Leakage Prevention tools, Antivirus solution shall be implemented.
-

12.0 Network Level Security

- KRBL network at all levels (LAN, WAN) shall be designed in such a way that no foreign computing resources shall be automatically connected.
- All temporary connections to external agencies within the KRBL or from outside using VPN shall be through Change Management Process. List of all such temporary outside connections shall be maintained by NOC team and requirement shall be reviewed by CIO at least once in a month.
- Host to Host connectivity shall only be based on a specific requirement

13.0 Database Level Security

CIO / IT Head shall designate Database Security Manager, who shall ensure Database access is documented for each critical application with proper approval.

26/04/2023

14.0 Preventing execution of unauthorised software

- Users shall not have authorization to install or uninstall any software (licensed, unlicensed, evaluation version, shareware & freeware) on operational system.
- IT support team is responsible for installation or un-installation of all software from operational system.

15.0 Physical Security and Environmental Controls

- Data Centre is to be audited annually to ensure compliance of environmental parameters viz. Power, Air Conditioning, Fire proofing and cleanliness.
- Asset Users/Custodians and Owners shall ensure minimum level of environment parameters as required by OEMs of respective assets are implemented and maintained. Performance shall be assessed periodically through preventive maintenance.
- Physical Access to KRBL's Data Centre (DC), Disaster Recovery (DR) Site or any other central server hosted location even in case of outsourced locations shall be based on requirement and authorization process by Asset Owners. Record of such access shall be maintained for a period of at least 6 months. These locations shall be categorized as Critical Locations.
- All Critical Locations shall be covered through CCTV systems and such footage shall be stored for a minimum period of 1 month.

16.0 Securing Customer data

- Customer data shall be made available to employees only on "need to know and need to do" basis and shall be controlled through username & password-based access.
- Customer data shall be shared to partner organization for 3rd party products only after authorization from customers.
- Sharing or storing of Customer data at Outsourced location shall be made only after Non-Disclosure Agreement and Service Level Agreement is signed with relevant confidentiality clauses.

17.0 Application Security

- All Critical applications shall follow principles of secure development, segregation of duties, Application Security Audit, Source Code Audit (if not a standard product).
- Asset Owner shall create document briefing the features of security controls implemented and placed to CIO as part of go live document.

18.0 Creating Awareness

- CIO/ IT-Head office shall coordinate to create awareness about Cyber Security amongst employees through HR, IT of the KRBL.
- At least one target campaign per Quarter shall be executed using SMS, Email, Intranet, Posters and Contests.

19.0 Internet Access

Devices with direct Internet access (which bypass the firewall security) are not allowed to connect to KRBL's network as user end points.

26/09/2023

20.0 IS Outsourcing

- Asset owner shall be accountable for any event occurred at partnered arrangements.
- Outsourcing shall be based on assessment of internal capabilities, cost of acquisition & operations and general industry level best practice.
- Partner needs to assure KRBL about their risk compliance through Audit Reports, industry level security standards.
- KRBL shall have full rights to conduct Audit of outsourced environment through internal or 3rd party resources. This clause shall be necessary part of all outsourcing agreements.
- In case, KRBL outsources asset management to technical expert agency/vendor agency within their premises, the agency's personnel shall also be part of continuous surveillance, NDA and SLA driven controls.

21.0 Data Leak Prevention

- Customer data collected through Business process, all spreadsheets, word processing files and database backup/ exports shall be considered classified.
- DLP solution should be implemented to monitor all users data activity.

22.0 Ethical Hacking, Honey pot

Ethical Hacking, creating honey pots shall be employed only after ITSC approvals.

23.0 Baseline Controls

Control	Parameter	Maintained Through	Document
Inventory Management	Applications	CIO / IT Head /ITSC	Annexure-1
	Assets	Asset Owner	Annexure-2
	Centralized Control	CIO / IT Head /ITSC	
	Patch Management	Manual, Automated	
	Exception Authority	Head-IT, CIO, ITSC	
Environment Control	Physical Security	Guards, Biometrics, CCTV	
	Hosting Environment	Building Management System	
	Network Architecture	CIO / IT Head /ITSC	

26/04/2023

Network Security	Network Assets	Manual, Automated	
	Configuration	Audit	
	Wireless Access	Change Request, MAC, Physical IP	
	Authorization	Manual, NAC	
	Unauthorized Device	Detect, Domain-AD, SIEM	
	Unusual Activities	SIEM	
	Boundary Defence	Firewall, Proxy, IPS, IDS	
	Patch & Configuration	Audit	
Application Security	Source Code Audit	Optional	
	OEM Assurance	SLA	
	Security Requirement	Asset Owners	Annexure 3
	Development, Test & Production System	Separate systems	
	Remote Wipe Solution		
	New Technology	Risk Assessment before induction	
Patch Management	Inventory of Patch Requiring systems	Asset Owners	
	Measurement & Tracking	Manual, Automated	
	Audit	VA/PT/ APPsec /RCA /Secure Configuration	

26/04/2023

User Access Control	Encryption of sensitive data at Rest	Legal and standard Compliance	
	Encryption of sensitive data in transit	VPN, IPsec, SSL	
	No admin rights on endpoints	Endpoint Admin through Endpoint Security SW	
	Centralized Controls	Endpoint Admin through Endpoint Security SW	
	Privilege Monitoring	End Point security SW / CASB	
	Invalid Logon Lockout	Three	
	Dormant Password Expiry	60-90 days – through Application	
	Abnormal Logon Alert	Time, Place abnormality	
Customer Authentication	Secure Authentication system	Policy	
Secure Mail Messaging	Own	SMTP Gateway, 2 Factor, Mail Gateway Security App	
	Partners	SMTP Gateway, 2 Factor, Mail Gateway Security App	
Vendor Risk Management	Accountability	NDA / Outsourcing Policy	
	Legal, Policy Compliance	NDA, Continuous Surveillance	
Removable Media	Policy definition	Part of Cyber Security policy	
	Limit Media & information Types	AV, Manual & Active Directory Services	
	Auto Scan for Malware	Antivirus Solution	
	Authorization	Blocked by-default	
Real-time Defence	Robust Defence	Antivirus Solution for all Assets & Mail Gateway Security for Messaging, DLP & CASB and Firewall for Web-access control	
	White listing	Domain & Mailing Solution	
Anti-Phishing	Service subscription	Mail Gateway Security service subscription- managed by internal team	

26/04/2023

Data Leak Prevention	Identification	Policy Configuration	
	Prevent	DLP Solution, CASB, AV-solution, Manual	
Audit Logs	Generation, storage and Analysis	SIEM & Internal NOC	
VA/PT	Periodic Audit	As per KRBL's IS Policy	
	Reporting	ITSC (Calendar Item) / Top Management	
	Participation in Drill	CIO / NOC Team	
Incident Management	Plan	Manual Analysis	
	Reporting & Lessons	RCA to ITSC/ top management	
	Recovery	BCP	
Forensic	Tie-up	External Agency – need base	
Awareness	Policy	Awareness Policy	

24.0 Cyber Crisis Management Plan

DETECT:

Following shall act as triggers in declaring CYBER CRISIS by CIO / IT-Head

- Incident of attack detected by NOC, Employees, Partners, third party agencies
- Discovery of compromise through outside agencies and authorities (Media, Customer, Regulators)
- Alert issued by support group & organization or news items

Severity of incident shall be classified as Major or Minor category. Major Incident shall be categorized so, if there is high probability of financial and/or reputation loss.

RESPONSE:

Timeline	Action	Sub-Action	By	Additional Point
Within 30 Minutes	Communication	Meeting of ISWC	CIO/IT-Head	
Within 2 Hours		To ITSC members	CIO/IT-Head	For Major Category
Within 24 Hours		To Cert-in	CIO/IT-Head	If attack on KRBL's systems
Within 24 Hours		To Customers & Employee's	Asset Owner	After ITSC approval
Within 2 Hours	Action	Response Action points shall be finalized	Asset Owner	After ISWC approval

26/04/2023

RECOVERY:

Timeline	Action	Sub-Action	By	Additional Point
Within 2 Hours	Isolation	Affected Asset	Asset Owner / Network Manager	If it is estimated system is having some degree of vulnerability
Within 4 Hours	BCP	Activate	Asset Owner	
Within 24 Hours	Log Collection	Affected Asset	Asset Owner/ NOC	

CONTAINMENT:

Timeline	Action	Sub-Action	By	Additional Point
Within 48 Hours	Learning	RCA	Asset Owner	
Within 48 Hours	Reporting	To RBI	CIO/IT-Head	
Within 48 Hours	Communication	Media	CIO/IT-Head	If Required by Regulators & ITSC
Quarterly	Review	Incident & Outcome	IT Steering Committee / Management	

25.0 Glossary

S No.	Abbreviation	Description
1	CSP	Cyber Security Policy
2	CIO	Chief Information Officer
3	IT	Information Technology
4	IPR	Intellectual Property Rights
5	IDS	Intrusion Detection System
6	IPS	Intrusion Prevention System
7	LAN	Local Area Network
8	DDOS	Distributed Denial of Service
9	DLP	Data Loss Prevention
10	WAN	Wide Area Network
11	VPN	Virtual Private Network
12	SOC	Security Operations Centre
13	NOC	Network Operations Centre
14	VA	Vulnerability Assessment
15	PT	Penetration Testing
16	ADC	Application Development Controller
17	DNS	Domain Name System
18	ITSC	IT Steering Committee
19	ITWC	IT Working Committee
20	UAT	User Acceptance Test

26/04/2023

26.0 Other References

S No.	Clause	Description
1	KRBL/IS/POL/ISP	KRBL-00-Policy-Information Security_v1.1
2	KRBL/IS/PROC/HRS	KRBL-01-Procedure-Human Resource Security_v1.0
3	KRBL/IS/PROC/AMP	KRBL-02-Procedure-IT Asset Management_v1.0
4	KRBL/IS/PROC/ACP	KRBL-03-Procedure-Access Control_v1.1
5	KRBL/IS/PROC/PES	KRBL-04-Procedure-Physical and Environmental Security_v1.0
6	KRBL/IS/PROC/OSP	KRBL-05-Procedure-IT Operations Security_v1.0
7	KRBL/IS/PROC/CSP	KRBL-06-Procedure-Communications Security_v1.0
8	KRBL/IS/PROC/SRM	KRBL-07-Procedure-Supplier Relationship Management_v1.0
9	KRBL/IS/PROC/IMP	KRBL-08-Procedure-IS Incident Management_v1.0
10	KRBL/IS/PROC/CGM	KRBL-09-Procedure-Change Management_v1.0
11	KRBL/IS/PROC/BCP	KRBL-10.a-Procedure-IS Aspects of Business Continuity Management_v1.0
12	KRBL/IS/PROC/DRP	KRBL-10.b-Procedure-Disaster Recovery_v1.0
13	KRBL/IS/PROC/CP	KRBL-11-Procedure-Compliance_v1.0
14	KRBL/IS/PROC/FRW	KRBL-12-Procedure-Firewall_Policy_v1.0

********** End of Document **********

26/04/2023