Cyber security Policy for HM Pharmaceutical & Medical Supplies

Objectives

This cyber security policy outlines the measures and guidelines to safeguard the information assets of Himalayan Marvels Pharmaceutical and Medical Supplies, a medicine supplier vendor based in Phuntsholing Bhutan with its office at Thimphu. The primary objective of the cyber security policy is to protect sensitive information, ensure integrity and availability of data, and mitigate cyber security risks.

1. **Information Security Responsibilities**
   All employees are responsible for safeguarding sensitive information and follow guidelines outlined in this policy where ever possible. Incremental measures will be implemented to fully make the company cyber secure in the long run.
   The CEO of the company will also look after and enforce cyber security of the company. In his unavailability, or on secondment, the Competent Person will be the Information security officer.
2. **Data Privacy:** HMPAMS is committed to respect personal and partner companies' data privacy. The HMPAMS will work towards ensuring that personal and partner data are secure through awareness, trainings and support from relevant partners and organizations. HMPAMS will identify measures for personal data processing and ascertain activities towards its mitigation.
3. **Access control**
   Sensitive information will be handled by the CEO alone and the CP if and when required, following policy of least privilege for user access to systems and data.
   Under no circumstance will sensitive information be handled by temporary or part time staff.
   Review updates user access permissions based on job requirement regularly.
4. **Password Security**
   Use strong unique password for all users account.
   Plan to implement Multifactor authentication (MFA) for logging process for additional security.
5. **Network Security**
   Change default usernames and passwords on network devices;
   Regular updatation of network devices and router and firewalls;
   Use of secure wireless network using WPA3 encryptation;
6. **Data Encryptation**
   Plan for long term data encryptation using HTTPS for sensitive data in transit;
   Plan to store sensitive data and sensitive information secure through encryptation in the long run.
7. **End point security**
   Install and regularly update antivirus and anti-malware software on devices;

All devices to have latest security patched in the long run;

8. **Physical Security**
   Restrict physical access to critical hardware;
   Securely store and dispose physical records containing incidents, including phising attempts.
9. **Training**
   Initiate cyber security training and awareness for employees regular-temporary, part-time and full time. Staffs are trained on data privacy measures, Educate employees on identifying and reporting security incidents, including phising. Include budget to hire expert for staff training on cyber security.
10. **Incident response**
    Develop an incident response plan outlining steps to be taken in the event of a security incident
    Establish a reporting process of security incidents as per the Royal Government's guideline and as per the principal company's needs.
11. **Personal data**
    Preserving individual autonomy in terms of data collection, use and share are respected; ensuring data privacy and personal information is not exploited or misused without consent. Further, data privacy are taken into account during procurement and distribution process.
12. **Principle company data security**:
    Seek support in the form of trainings, cost of training etc. from principle companies to secure partnering companies data safely.
13. **Compliance:**
    Remain informed about and comply with relevant local laws, rules and regulations.
14. **Data inventory and Backup:**
    Critically important data should be backed up regularly and stored in secure place. Regularly back up critical data and ensure backups are stored securely. An inventory of data and their associated classification is formalized and maintained up to date.
15. **Vendor Security**:
    Assess the security practices of third-party vendors and service providers. Ensure that vendors with access to sensitive data adhere to similar security standards.
16. **Compliance:**
    Stay informed about and comply with relevant laws and regulations, within the country and international, related to data protection and cyber security.
17. **Security Audits:**
    Conduct regular security audits and assessments to identify and address potential vulnerabilities.
18. **Mobile Device Security:**

Implement mobile device management (MDM) solutions to secure and manage mobile devices used within the organization.

19. **Documentation and Review**: Maintain documentation of cyber security policies and procedures.
20. Regularly review and update the cyber security policy to adapt to evolving threats and technologies.

By adhering to this cyber security policy, we aim to create a secure environment for our information assets, protect the interests of our customers, and maintain the trust and confidence of all stakeholders.

Bivatsu Giri
Chief Executive Officer
HM Pharmaceuticals and Medical Supplies
NPPF Colony, Phuentsholing, Bhutan
Date: 27th November 2023