<u>BUSINESS APPLICATION/INTRANET AND INTERNET ACESS AND SECURITY POLICY</u>

Table of Contents

1.INTRODUCTION

Harrisons Malayalam Limited computer network introduces new resources and new services through Intranet, Business applications and Internet connectivity. This connectivity not only results in new capabilities, but also in new risks and threats. This document formally defines our official policy regarding Business application/Intranet and Internet security in response to potential risks. All Internet users are expected to be familiar with and to comply with this policy.

Unless specifically stated otherwise, all statements and policies will apply to the Business applications and the Internet.

For the purposes of this document the Internet is defined as a worldwide “network of networks” using Transmission Control Protocol/Internet Protocol (TCP/IP) for communication. The Intranet is defined as Harrisons Malayalam Limited “internal infrastructure” connecting our facilities by using TCP/IP.

1.2Purpose

HML is responsible for properly securing the data maintained in and transmitted by its computing systems and telecommunications networks. In addition, HML is committed to preventing the occurrence of inappropriate, unethical or unlawful behaviour by any of its users. These responsibilities are not only mandated by the facility’s business interests but also by legal and ethical obligations concerning the welfare and privacy of its customers and business partners. This Business application/Intranet and Internet Security Policy and its strict enforcement is an important and necessary part of the overall security strategy.

1.3Scope

The scope of this policy includes the following information:
Security threats
Management controls required for access security;
Information confidentiality and protection;
Expectation of privacy;
Contacts for security issues and questions;
Backup, recovery, and change management;
Periodic reviews.

The components outlined in this document focus on connectivity issues associated with Harrisons Malayalam Limited host computers, PCs, routers, terminal servers, and other devices that support access to the Intranet and to the Internet. The scope of this document does not include facility-specific security policies, application security, and non-network security.

The Business application/Intranet and Internet Security Policy applies to all Intranet/Internet users (individuals working for HML, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners and vendors) who access the Intranet or Internet through the computing or networking resources. Harrisons Malayalam Limited IT systems users are expected to be familiar with and to comply with this policy.

1.3Consequences of Violations

Violations of the applications and Internet Security Policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination. Additionally, the HML may at its discretion seek legal remedies for damages incurred as a result of any violation. HML may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the HML network is approved, the potential systems user is required to read this Business application/Intranet and Internet Security Policy For questions on the Business application/Intranet and Internet Security Policy, contact the Information Technology (IT) Department.

2.SECURITY THREATS

Internet connectivity presents HML with new risks that must be addressed to safeguard the facility’s vital information assets. These risks include:

2.1Unauthorized Access

Internet connectivity increases the risk of unauthorized access to HML systems and files. The scope of this risk includes the servers supporting HML connectivity as well as other systems that are connected to the same physical or logical network as these servers. Malicious activities that may result include:

Disclosure of confidential information that results in loss of customer confidence, and/or legal action in situations involving customer privacy and regulatory matters.

Unauthorized creation or modification of information that results in loss of data integrity. Corrupted data may also adversely affect business decisions making on financial, strategic, or competitive issues.

Denial of service or operational delays due to attacks that jam or disable network components, rendering the network unusable. This threat to the timeliness of information and information processing services may prevent HML from meeting critical deadlines and impact the quality of our products and services.

Viruses introduced intentionally by a malicious individual or accidentally through files downloaded from the Internet may degrade service and system availability network-wide. They may also result in the loss or corruption of information required to maintain vital operations or support corporate-wide business decisions.

2.2Misleading or False Information

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is out dated or inaccurate.

3.BUSINESS APPLICATION / INTRANET/INTERNET SERVICES

Access to the Business application/Intranet and Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

3.1User Services

connecting to the Internet Access to Internet services will be provided by discrete, designated and secured sources. Each source will maintain the appropriate firewalls and filters. Networked workstation connectivity through separate analog lines and modems is prohibited. At no time should networked workstations be connected both to the Internet via a modem and to the HML network.

Network administrators will ensure that appropriate router and filtering systems are in place to technically support the access requirements defined by this policy.

Business application /Intranet/Internet Services Availability Every attempt will be made to maintain availability of Business application /Intranet/Internet Services 24 hours a day, seven days a week. These services are being provided to support business activities; therefore, availability of Internet services for users between 8 AM and 7 PM IST on regular working days will have priority. Access at other times will depend on general system availability and scheduled maintenance activities.

4. ACCESS CONTROL AND SECURITY POLICIES

4.1Access Controls

All access to and from the Internet will be strictly controlled.

4.1.1 User Strong Authentication

All Internet users who attempt to enter internal networks as allowed by this policy must authenticate themselves through the authentication mechanism established by HML network. Authentication prevents unauthorized users from gaining access to internal systems. Authentication techniques may employ strong authentication devices.

Strong authentication techniques enhance password level authentication through various cryptographic and bi-directional data exchanges involving dynamically generated single use passwords and/or challenge-response techniques. User authentication must be used to gain access to the network for Telnet or FTP regardless of data classification level. In addition, passwords chosen by the users must meet the requirements of the Password Policy.

Under no circumstances should users establish Internet or other external connections that could allow unauthorized outsiders to gain access to HML systems and information. These connections include, but are not limited to, multi-computer file systems, Internet home pages, and FTP servers.

4.1.2 Traffic Flow

Unauthenticated (through strong authentication) in-bound traffic from the Internet will not be permitted except for E-mail and access to public web servers. Only authenticated users who have been approved by the IT department for access to their internal networks will be allowed in from the Internet.

4.1.3Dial-up

Networked workstations should not be connected to separate analog lines or modems unless required for performance of business functions and specifically authorized by the facility's IT department.

At no time should networked workstations with modems be left in an accessible state that could potentially allow unauthorized access. Direct remote dial-in to the Intranet is not allowed.

4.1.4Physical Security

Physical access security measures must be taken to protect against the intentional or accidental intrusion by unauthorized individuals into any area where sensitive information may be readily accessible. Questions or issues should be brought to the attention of the IT department.

All vital system hardware must be physically protected against unauthorized access. Violations should be brought to the attention of the IT Department.

4.2Information Classification

Information Classification Information must be classified according to the most sensitive detail it contains. Any questions about classification should be addressed to the IT Department. The following levels are to be used for classifying information:

Level 1 Confidential Information:
This class represents important and/or highly sensitive material that is confidential according to the existing laws of India. Unauthorized disclosure, modification, or destruction of this information could cause serious damage to HML and its customers.
Examples of Level 1 information includes personnel information, payroll information, system access passwords, information file encryption keys, and all customer information.

Level 2 HML Information:
This class represents information important to the HML. Its destruction and/or modification could result in serious and irreparable loss. This information must have controls to ensure its integrity and accuracy. Its use is therefore subject to certain restrictions.
Examples of Level 2 information includes accounting, budget, HML-wide memos, local operations manuals, and HML policies and procedures.

Level 3 Unrestricted Information:
This class represents information that does not fall into one of the above classifications and is appropriate for all HML personnel in addition to the general public. This information is not considered confidential, and its disclosure, modification and/or destruction do not need to be controlled.
Examples of level 3 information include general correspondence, newsletters, articles, speeches, photographs, brochures, advertisements, displays, and presentations.

4.2.2 **Information Responsibilities**

All Level 1 and 2 information must have an owner. Originators of information communications must determine appropriate information classifications and are the information owners. Recipients of data and information assume responsibility for subsequent handling of data and information in a manner consistent with the originators classification.

Information owners must determine appropriate information classifications, maximum acceptable unavailability, resource protection measures, and user access requirements. Level 1 and 2 information should be marked with its classification and with all other relevant handling instructions for all transmissions. Information owners must review all level 1 and 2 information annually and re-certify their classification.

(Note: The information ownership role should not be confused with legal ownership. All HML information is the property of the HML.)

4.3 Information Protection

4.3.1Message Source Authentication and Integrity

Message source authentication ensures that information or data in transit is received from the named source. This is achieved with digital signatures. Digital signatures indicate that a message came from the person it is alleged to have come from.

Digital signatures not only indicate that a message came from the person it is alleged to have come from, they also indicate that a message has not been altered during transit. Digital signatures should be used whenever message integrity is considered important.

This can be used when communicating data at all classification levels. This feature should be available for HML internal communication in the near future.

4.3.2Encryption

The following data transfers over the Business application/Intranet and Internet are prohibited unless the data is encrypted by a HML approved public or private key standard:

HML information classified as Level 1,
Credit card numbers, telephone calling card numbers, Log-in passwords and other parameters that can be used to gain access to goods or services.
In addition, Level 2 data sent over the Internet must be encrypted. It may be unencrypted on the Intranet.

4.3.3 Virus Detection

All software downloaded from non-HML sources through the Intranet or Internet must be screened with virus detection software before being invoked. The most current release of the virus detection software and definition files must be used. These updates will be distributed as soon as they are released. When available on the market, virus detection software with the capability of checking Business application/Intranet and Internet E-mail attachments, web traffic, and FTP must be used in addition to the regular scanning of disk drives on the users' workstations.
Automatic scanning for virus must be installed on all PCs and servers accessing the Internet and should not be turned off by the user. In addition, all users must periodically scan their PCs and take responsibility for ensuring that all files sent out are free of virus infections.All HML's networked workstation are protected with Anti Virus software and this should never be disabled.Network

workstations without anti- virus software should contact the IT department immediately.

4.3.4 Prohibited Usage

Activities that are strictly prohibited include, but are not limited to:
Any unauthorized, deliberate action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration;
Wilful or negligent introduction of computer viruses, trojan horses or other destructive programs into HML systems or networks or into external systems and networks;
Unauthorized decryption or attempt at decryption of any system or user passwords or any other user’s encrypted files;
Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to a computing system or network.
If you have any questions about Prohibited Usage, contact the IT Department.

4.4Reporting Security Problems

4.4.1Lost or Stolen

It is the responsibility of the user to report any known or suspected breach of security, such as passwords or other system access control mechanisms to the IT department.

4.4.2System Problems

Unusual system behaviour such as missing files, frequent system crashes, or miss-routed messages, should be immediately reported to the IT Department, who will refer the situation to the appropriate parties for investigation. These types of system behaviour may be related to virus infections or other security problems and must be promptly reported and investigated. The specifics of security problems should not be discussed except on a business need-to-know basis.

4.4.3Confidentiality Violation

If proprietary information (Level 1 or Level 2 information as defined in section 4.2.1) is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IT Department must be notified immediately.

4.4.4Security Testing

Unless authorized by the Corporate Security Authority, users are not to test the security mechanisms at the HML or at Internet sites. If users probe security mechanisms, alarms will be triggered and resources needlessly spent to track the activity. This could result in revocation of access rights and/or disciplinary action up to and including termination.

4.4.5 Virus Infection

Immediately report any virus infections or attacks to the IT department.

4.5 Periodic Reviews

4.5.1Security Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with security policies.

4.5.2Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of security policies. These reviews may result in the modification, addition, or deletion of security policies to better suit HML information needs.

5.REFERENCES

5.1Confidentiality Laws and Procedures

For violations of the laws related to computer crime and systems security the iT department shall be informed and the IT department shall take immediate steps to inform the authorities under the law so as to take necessary steps to curb the same

5.2 Points of Contact

If you need assistance regarding the following topics related to Internet security, contact the IT Department for additional assistance: