IDEA Cellular Information Security

Contact Centre

Information Security & Privacy Policy

Document Information

Author	Pradeep Keith Fernandez
Reviewers	Sunil Varkey, K A V Prasad
Approver	Prakash Paranjape, Mallikarjuna Rao
Effective Date	15th Sept 2012
File	IDEA Cellular – Contact Centre Security & Privacy Policy.doc

1 Distribution List

Sl. No	Distributed to	Issue Date	Media	Issued by	Remarks
1.	All IDEA Contact Centre's and their Employees	15th Sept 2012	Electronic	Idea IT Security Team	

2 Change History

Version #	Release Date	Sections Changed	Change Description
0.1	1st Feb 2012	Initial Draft	Draft Version
1.0	15th Sept 2012	All as per comments from Contact Centre's and Service Delivery Team	1st Version

Disclaimer

This document is intended to assist all Contact Centers and Third Parties providing any service or product to IDEA Cellular, required to undertake reasonable measures to secure IDEA information and to comply with IDEA Security Policy, besides such security notification issued by the State and/or any regulatory Authority. Each Contact Center must read and accept this document and any addendums for individualized adaptation to the service provided to IDEA or its partners and affiliates. While it has been drafted to provide accurate and authoritative assistance in the development of necessary policies, procedures, and forms, it is not a substitute for legal advice and users should consult experienced counsel for individualized and ongoing guidance regarding the specific and evolving application of this policy to their practice, as well as for other IT Act 2000, TRAI, DoT and other related regulatory contractual and compliance concerns.

Table of Contents

3 Contact Center Information Security

3.1 Introduction

IDEA Cellular Ltd (ICL) recognizes that information protection requires close cooperation between ICL and its suppliers, vendors, partners, and customers. This document outlines ICL's security policies designed to safeguard ICL Business, employees, customer Information (ICL information), as well as information belonging to Contact Centers, from unauthorized or accidental access, modification, damage, destruction, or disclosure.

3.2 Scope

This policy addresses technical security, Privacy and compliance concerns with respect to ICL contact center security, secure usage of IDEA data and general connections into the ICL internal network from Contact Centers. The basis for the control objectives and controls is compliance with applicable law, regulation (especially IT ACT 2000 and its subsequent ammendments, UASL Security Requirements, ISO 27000 and ICL's general policies & Values and the Information Security & Privacy policies). However, most of this document's procedures go beyond technology concerns and have wider applicability. Data can exist in the following forms:

- Data stored on devices
- Transmitted over networks
- Printed out
- Written on paper
- Sent by FAX
- Stored on disk
- Spoken in conversation over the phone

ICL reserves the right to modify or amend this policy at any time, at ICL's sole discretion. ICL may periodically update its security policies based upon newly identified vulnerabilities and threats and published to all constituents through its website or other communication channels. In addition, ICL already has an extensive network of existing Third Parties and business partners Connections with additional joint risk. To minimize this residual risk, existing & new Contact Centers should be brought in line with the then current information security policy. All Contact Centers should have all gaps identified, then brought into compliance or mitigated through proper risk management process.

Any exceptions or non-compliance to this policy should be discussed and mutually agreed for a specific period of time in writing between the IDEA SPOC requesting the exception and Idea Information Security team.

3.3 Definitions and Terms

Certain terms are used throughout this policy; in order to avoid misinterpretation, several of the more commonly used terms are defined below.

ICL Information: Information is an asset like other important business assets, which, has value to ICL and consequently needs to be suitably protected. Information can exist in many forms which can be data stored on devices, transmitted across networks, printed out, scanned, stored on disks, etc.

Contact Center: A call centre or contact center either inbound, outbound and backend providing services to IDEA for the purpose of receiving, transferring and attending to a large volume of queries, service related resolutions and complaints by various means including but not limited to telephone, IVR, web etc.

Basic Contact Center Connection: A site-to-site connection between Contact Center network and ICL internal network that requires Least Access firewall rules and NAT of ICL's internal addresses. Used for outbound-initiated connectivity into the Contact Center network, or a specific set of inbound IPs/ports/protocols acceptable to ICL (not typically UCA/NetBIOS/SMTP/DNS which require special security audits and controls normally associated with a Trusted Contact Center Connection).

DR: Disaster Recovery: Corresponds to the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to ICL after a disaster.

Agent - a person whose phone or mails are programmed to receive Call Center calls / mails (i.e. Call Center staff or representative)

Manager/Supervisor/Team Leader – A person who manages agents at a call center for escalation calls and presentation of reports to IDEA

ITC: Information Technology Center – a Trusted Center with additional management controls and oversight sponsored by ICL to service multiple Technologies and services

Housing: Contact Center that stores or processes ICL data such as data processing applications, data center services and backup tape storage facilities. Housing includes ICL data storage whether accessible to the Internet or not.

Least Access: The minimum required access rules necessary to achieve function required; used to describe "locked-down" firewall rules.

NAT: Network address translation; used to change ICL internal addresses to numbers routable on the Third Party's network; required for Basic Contact Center connectivity.

Remote VPN: Individual Internet-based access to the ICL internal network using two-factor authentication such as SSL-VPN or IPSec. Because a token is required, it is not suitable for access by automated processes.

Trusted Contact Center Connection: A Contact Center network connected over IDEA MPLS network to ICL internal network and entry restricted by suitable security controls.

Third Party: Non-ICL vendor, supplier, partner, contractor, service provider, or customer with connectivity to ICL's internal network or access to ICL data via the contact center. This includes joint ventures without majority IDEA ownership.

3.4 Organization

The requirement for a security organization as regards to this policy is to

- Ensure security and privacy of ICL data
- Adherence to various regulatory and legal compliance requirement
- The identification of risks related to external parties.
- A similar responsibility is addressing security when dealing with "customers" (e.g., Customers and other constituents).
- Addressing security in Contact Center agreements to ensure reasonable coverage of all relevant institutional security requirements
- Higher service availability due to better Information Security Posture

IDEA SPOC: Every Contact Center should have a SPOC or designated person from the Service Delivery team located at the contact center responsible for owning the business relationship and overall performance including adherence to compliance and security requirements. The IDEA SPOC should be guided by local business definitions, legal or regulatory requirements and the specifications of the IDEA Information & Telecom Network Security Policy and security program.

Control: Personnel, physical, software, information asset ownership, access control and identity management responsibilities.

Physical Security: Access to workplace, computer rooms, systems, and media/documents

IDEA Business Legal Team: Approves contract as meeting IDEA and legal standards.

Master Services Agreement: reviewed and approved by the appropriate IDEA legal / Commercial department with necessary signatures from both parties.

IDEA Information Security Team: IDEA Information Security Team should act as the interface through Idea SPOC for all information security and privacy related queries that the Contact Center may have regarding IDEA Information Security policies and adherence to those policies. This team will be responsible for coordinating & conducting the risk assessment and periodic audits to validate the information security & privacy controls and adherence to Third party information Security Policy for Contact Centers.

System Security and IDEA Metrics: System and application configurations and vulnerabilities with periodic metrics (refer to Appendix C) reporting to the IDEA Security team

Business Access and Network Security: Type of Contact Center Connection (Basic/Trusted), network access details and termination dates Need to revalidate this

Contact Center Manager: A designated individual at the vendor responsible for the ICL-Contact Center relationship.

Contact Center Security SPOC: Designated by the Contact Center Manager with notification to the ICL Sponsor and IDEA Information Security Team to supervise and coordinate security activities within the organizations. Assumes role as primary point of contact with ICL in case of security incident response. And periodic communications on the security posture and metrics.

3.5 Establishing Security Requirements

This information security policy document is organized in three sections. Based upon ICL assessment of business access needs, then language addressing one, two or all three sections should be included in Contact Center agreements.

Section 4. **General**: All Contact Centers must comply with General security requirements

Section 5. **Data and Application**: Additionally applies if Contact Center is Housing ICL data

Section 6. **Network Connectivity**: Additionally applies if the Contact Center has direct access to ICL networks

The business need to access ICL data, networks, and systems is a decision based upon assessment by the ICL Sponsor and IDEA Information Security Team, Contact Center status, work & services performed, number Circles served and type of access.

4 General Security Requirements

4.1 General Audit

Data in any form created, modified, transmitted or stored on ICL systems or generated while supporting ICL is deemed to be the property of ICL. ICL reserves the right to audit / review "Information Systems" on a periodic basis to ensure compliance with this Policy.

The Contact Center upon request must provide copies of relevant security policy, process, and procedure documents to ICL for review and audit purposes. ICL should review and recommend reasonable changes, and supplier must amend the policies or respond with mitigating controls and responses.

Audits will be conducted to ensure integrity, confidentiality and availability of ICL data, IT and telecom network assets, to ensure conformance to ICL security & Privacy policies, investigate possible security incidents and to monitor user or system activity where appropriate.

In addition to any audits provided for in IDEA contractual agreements, the Contact Center must permit IDEA to request and/or perform, at the expense of IDEA, security assessments each year, including but not limited to, review of policies, processes, and procedures, on-site assessment of physical security arrangements, network, system, and application vulnerability scanning, and penetration testing if required

Frequency of audit may change based on the current & historical incidents, trends, variation in security postures, changes to the infrastructure, compliance / regulatory requirement and new threats

All Contact Center Workers with access to IDEA networks and data must receive accept and sign the Acceptable Use Policy and Agreement. And between the organization Non Disclosure Agreement

should be signed before transferring or accessing any data

Periodically risk should be assessed and a risk register (refer Appendix D) should be maintained by contact Centre SPOC

The Contact Center Manager should ensure that Contact Center personnel added to the IDEA account (in-processing) and removed from the IDEA account (out-processing) are completed in a timely (5 working days), consistent manner auditable by IDEA.

All IT Audit will primarily based on the ISO27001 framework and any changes will be communicated in advance

The Audits will

- Review policies and procedures and verify the adherence to these policies and procedures.
- Assist and coordinate with external auditors to provide an effective and efficient audit function within ICL.
- Employ knowledgeable, competent personnel with experience in information security and privacy controls
- Initiate / Plan audit based on business requirement, prioritities, potential or previous history of threats & Vulnerability

Use of External Audit Agencies

The IT Security team may use outside Consulting and Audit firms to perform certain audit functions outlined in this and any other policy and procedures promulgated by ICL.

4.2 Personnel

All employees working on ICL information should have undergone background checks prior to induction to team. Background check information should be available for audit if necessary. The extent of background check required will be based on the type ICL information access and handling and could vary from address verification to criminal background verification.

Contact Center Manager must ensure employees are aware of the fact that they are not entitled to privacy protection in the use of their company computers and networks where ICL data is processed, stored or displayed, and these resources may be monitored. Contact Center Manager must define a formal process for responding to a security & Privacy policy breach by Contact Center ICL Workers.

The Contact Center must have designated staff whose job responsibilities include information security, privacy and information risk management.

All contact centre employees accessing ICL data should be aware of the sensitivity and the approved usage of the same and related responsibilities (ex. Call records, customer information, credit card information etc). This should also be included in the individual acceptance document
All Contact Center ICL Workers with access to ICL networks and information must receive a copy of the Acceptable Use of ICL Information Resources (see document in Appendix) and Contact Center security policy and legal compliance developed by the Contact Center as part of their induction program. Contact Center must maintain and audit the inventory of individual acceptance of this policy.

4.3 Data Storage and Handling

4.3.1 Contact Center must at a minimum follow the ICL *Data Classification Guidelines* (see Appendix) directives when storing ICL data. The following best practices meet these requirements.

4.3.1.1 Follow a clear desk policy to securely store ICL documents. The Contact Center security team must audit and confiscate unattended documents.

4.3.1.2 Contact Center employees should not have access laptop, Smart phones, PDA to any ICL information through email or network access without adequate protection to ensure confidentially due to loss of device, possibility of storing and forwarding sensitive information to external sources

4.3.1.3 Passwords and challenge response answers must not be stored in clear text.

4.3.1.4 Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal, all ICL *Confidential* and *Restricted* information must be physically destroyed, or erased using tools for hard disk overwrite provided on ICL Securing Your Computing Environment Support Central).

4.3.1.5 All waste copies of ICL *Confidential* and *Restricted* data generated in the course of copying, printing, or otherwise handling such information must be destroyed in a secured manner

4.3.2 Do not make copies of ICL *Confidential* or *Restricted* information without the permission of the ICL information owner.

4.3.3 ICL data at the Contact Center in any form must not be stored or replicated outside the Contact Center without special agreement; obtain approval from the ICL Sponsor before transmitting ICL data to a subcontractor or any non-ICL entity. The Contact Center Manager must maintain an inventory of the non-ICL entities that are receiving the data, the purpose of the data transmission, the transmission and encryption/protection method or protocol, the data that is transmitted and the ICL approver and IDEA Information Security Team who has authorized the transmission with these controls.

4.3.4 Upon conclusion or termination of the work agreement, the Contact Center must provide ICL with copies of all ICL information maintained under the work agreement, as well as all backup and archival media containing ICL information.

4.3.5 Upon conclusion or termination of the work agreement, the Contact Center must use mutually agreed upon data destruction processes to eliminate all ICL information from the Contact Center systems and applications.

4.3.6 ICL data should not be stored in a portable devices and access to those devices should be blocked in all systems

4.4 Data Transmission

4.4.1 Contact Center must at a minimum follow the ICL *Data Classification Guidelines* (see Appendix) directives when transmitting ICL data. The following ICL best practices meet these requirements.

4.4.1.1 Email: ICL *Confidential* Information sent over mail must contain [Confidential] in the subject line and confidential information in attachments should be password protected when sent over email

4.4.1.2 Printed Delivery: Send ICL *Confidential* and *Restricted* printed information by trusted courier or registered mail with tracking approved by ICL.

4.4.1.3 Fax: Information classified as ICL *Confidential* or *Restricted* should not be faxed.

4.4.1.4 Phone: ICL *Restricted* information must not be discussed on speakerphones or during teleconferences unless all participating parties first confirm that no unauthorized persons are in close proximity such that they might overhear the conversation.

4.5 Laptops/Workstations

4.5.1 Contact Center is responsible for the infrastructure that supports user compliance with the *Acceptable Use of ICL Information Resources* (see Appendix). The policy applies to laptops, desktop PCs, Smart phones, Unix workstations, mainframe terminals and all other systems processing and storing ICL Information

4.5.2 Contact Center must maintain laptop and workstation security through demonstrated provisioning, Vulnerability Management, and antivirus processes. Personal firewall and anti-virus are required for all laptops. Laptop disks having ICL information should be encrypted and should have data leakage controls

4.5.3 Systems with direct access to the ICL internal network must follow quarterly reporting to the IDEA Information Security Team in the form of the ICL Information Security Metrics (refer Appendix C). They may be restricted or removed for compliance failure or compromise.

4.5.4 ICL data must not be stored on portable computing devices or through CD drives and access to portal devices should be restricted in all systems

4.5.5 All users should have unique user ID and strong authentication has to be enabled on all systems that Contact Centers have access to within IDEA and within the Contact Center where the IDEA application has the technical feasibility and feature / option available

4.5.6 If systems are shared with any other users, adequate security should be in place to ensure that any IDEA specific data is not stored locally on any endpoints such that data is accessible to others and users profiles are segregated by separate login ID's and separate environment for each user.

4.6 Incident Response

4.6.1 Contact Center Manager or Contact Center Security SPOC must maintain an up-to-date information security incident response plan including mobilization contact/call trees, bridge numbers, severity assessment, log recording steps, evidence collection and process diagrams.

4.6.2 The Contact Center should monitor all intrusions, attacks and frauds and report the same to IDEA as soon as the incident comes to light and ensure that incidents are adequately mitigated by taking necessary steps in terms of deloying additional controls and processes.

4.6.2.1 Contact Center Security SPOC must review test results of periodic drills with IDEA Information Security Team. Violation of ICL Information Security policies, virus/worm attacks, spam, data compromise, change failures, information leakage and physical asset loss must be covered.

4.6.2.2 Contact Center at the request of ICL, must provide copies of any log files maintained by

the Contact Center (including firewall, intrusion detection, system, and application log files) to support any investigation or legal action that may be initiated by ICL.

4.6.3 Contact Center Manager must notify and update the ICL Sponsor and/or IDEA Information Security Team without unreasonable delay of any actual or threatened unauthorized access, breach, disclosure or information or to the systems holding or providing access to such data. Final notification must include detailed incident log and root cause analysis within five days of closure that describes actions taken and plans for future actions to prevent a similar event from occurring in the future. The Contact Center IDEA Information Security Team must discuss process with ICL Security team, but expectation is within two hours of discovery and mutually agreed upon updates for agreed upon high-impact incidents.

4.6.3.1 Contact Center must report all occurrences of viruses, malicious code out breaks, Intrusion / extrusions not handled by deployed detection and protection measures, on any workstation or server used to provide services under the work agreement, to ICL without unreasonable delay. ICL expectation is within four hours or as negotiated with the IDEA Information Security Team.

4.6.4 Contact Center must first secure ICL approval of the content of any filings, communications, notices, press releases, or reports related to any security breach prior to any publication or communication thereof to any Contact Center. The Contact Center Security SPOC must maintain a well-understood reporting procedure for security incidents and train Contact Center ICL Workers on ICL contracts.

4.6.5 Contact Center should control and protect all potential vectors for information leak

4.7 Contact Center Workplace Security

4.7.1 Entry to the Contact Center area with ICL data access must be restricted to personnel authorized for access including an access termination procedure and periodic audit.

4.7.2 Visitor logbooks must be maintained which includes clear description of the visitor, arrival and leaving time, and ICL-relevant business purpose. A Contact Center employee must always escort visitors within the Contact Center area.

4.7.3 A security guard or electronic access control must protect entry to Contact Center area. Entry and exit logging are preferable. Software-based access control systems must be secured, have proper backups and be highly available. Entry logs must be maintained for at least six months.

4.7.4 Ensure all auxiliary entry points are secured. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained for at least one month.

4.8 Server and Equipment Room Access

4.8.1 All Server and equipment room doors must be secured to prevent access into the room unless otherwise authorized by the Contact Center Security SPOC.

4.8.2 Each computer room door must have signs on both sides indicating it is to be closed and locked with a contact to notify if it is found unsecured.

4.8.3 An identification badge reader must control all entrances into the computer room. Any other doors must be exit-only. The entrance and exit doors must be alarmed such that if left unsecured longer than one minute, the Security Office will be automatically notified. The Administration team must investigate the cause of the alarm, arrange to have it corrected, and notify the Contact Center Security SPOC of incidents.

4.8.4 Identification Badge Systems must generate a log of each entry. All door openings must generate a log entry, and every time the identification badge reader is used, it must log date, time, room location, and badge number.

4.8.5 Anyone needing badge access to any computer room must follow a defined procedure approved by the Contact Center Security SPOC including the badge holder's name, badge number, computer room location, reason access is needed, and termination date for fixed duration Contact Center ICL Workers. The Contact Center Security Office must not configure any badge for computer room access without being authorized by the Contact Center Security SPOC or designated team members.

4.8.6 Employment termination must result in badge access termination within a few hours agreed upon by the IDEA Information Security Team. The Contact Center Security SPOC must confirm that the badge access list is validated every quarter to verify those on this list still require access. Any discrepancies found must be corrected.

4.8.7 Badge access must only be given to individuals who require long-term access (those who are responsible for continuous administration or maintenance of the equipment located in the room). Visitors having business need confirmed by the Contact Center Security SPOC are allowed escorted access. If system access is required, the escort must have the technical security background to monitor any commands typed, or equipment added or removed. The Contact Center Security SPOC may allow badge access for short-term access under special circumstances if determined appropriate.

4.8.8 Anyone having badge access to a computer room must not give or loan their badge to another to gain access to a computer room.

4.8.9 Cameras and removable media drives should not be allowed in the data centre. Any exception to this should have prior approval from authorized personal

4.9 Consumer and Regulatory Compliance

4.9.1 All contact centers dealing with ICL information should be aware and comply with industry and regulatory policies applicable to ICL data and security controls such as TRAI regulations, DoT guidelines, IT Act 2000 and its subsequent ammendments and other applicable laws of the land.

4.9.2 Contact Center must not disclose market or otherwise contact ICL customers or employees/contractors outside of their work on behalf of ICL, either electronically or through other media, using information gathered from Contact Center web sites or ICL data.

4.9.3 If one of the above stated policies is in conflict with a governmental regulation, the issue must be presented to the IDEA Information Security Team for investigation and resolution.

4.10 Information Privacy

4.10.1 Contact Center employees should be aware about the sensitivity of the information they are handling and the related ICL policy and IT Act 2000 and its subsequent ammendments requirements

4.10.2 All required controls has to be in place to protect the information from disclosure or using for purpose other than purpose of collection and defined business objective

4.10.3 Any liability due to disclosure of information shared outside other than specified in the contract will be the responsibility of the Third party / concern contact Centre

5 Data & Application Security Requirements

5.1 In-house Security Assessment And Penetration Testing

5.1.1 A Contact Center Housing ICL Confidential or ICL Restricted data must have infrastructure security reviews performed by a Contact Center at least annually.

5.1.2 Contact Center must conduct regular periodic and change-related internal audits of networks and systems.

5.1.3 Contact Center must review with ICL all high & medium risk items identified through infrastructure reviews and audits (internal or external, security and otherwise) that Contact Center does not remediate within 10 business days.

5.1.4 The Contact Center upon request must provide copies of relevant security policy, process, and procedure documents to ICL for review and audit purposes. ICL should review and recommend reasonable changes, and supplier must amend the policies or respond with mitigating controls and responses.

5.1.5 ICL Security Metrics—report quarterly based on the nature of engagement through the IDEA Information Security Team of security defects and opportunities (contact IDEA Information Security Team for details and process). Ideally this should include the key security & privacy risk identified, effectiveness of the security & privacy controls, related deviations, planned / scheduled changes to infrastructure etc. During an audit if there is a found to be a discrepancy of data reported then the frequency of reporting these metrics may be increased accordingly.

5.2 Process Isolation and Architecture

5.2.1 ICL data and processes must be processed in separate systems from Contact Center running other process other than IDEA from data belonging to or accessed by other companies. Physical and logical architecture of the Contact Center should be segregated from non-idea processes.

5.2.2 At no time may ICL data be housed on a server shared by companies other than the contracting vendor. For example, a shared web server that is used by several companies and maintained by an Internet Service Provider must not be used to house ICL data.

5.2.3 Internet facing web servers must be dedicated to this task, and must not host internal (intranet) applications for the Contact Center.

5.2.4 Segregation of duties should be ensured for all access and activities

5.3 Trusted Contact Center Network Architecture

5.3.1 All current and new interconnections between the Trusted Contact Center network and any other network, including the Internet and other companies, should be managed by ICL and should meet ICL standards and requirements for these types of connections.

5.3.2 The Trusted Contact Center Network by default is a standalone group of subnets with no physical or logical connectivity to any network other than the ICL network. The business network of the Contact Center should not share layer-2 switches.

5.3.3 Firewall filtering rules are recommended between the Trusted Contact Center Network and the ICL network to limit the access from the Trusted Contact Center Network to only the systems needed to implement the business function. These filters should also ensure that all traffic destined for the ICL network originated on the Trusted Contact Center Network. Note: If total access to the ICL network is required then filters are not needed, but have proven useful during incident response. The use of filters should support the business need while providing only necessary access.

5.3.4 Separate VRF's will be provided for third parties to connect to the IDEA LAN via the MPLS or Internet. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication.

5.3.5 The address given to the Trusted Contact Center Network is dependent on the work being done by the Trusted Contact Center for ICL and the access needed.

5.3.5.1 If the work is being performed for a specific business or for network/compute management, then use addresses that are registered to the Contact Center but not publicly routed.

5.3.6 It is recommended that the interface between ICL and the contact center party be monitored for inappropriate activity using Antivirus, intrusion prevention/detection technology.

5.3.7 Physical access to the network devices (routers, hubs, switches, etc.) should be protected to allow access only by approved Contact Center staff.

5.3.8 The Trusted Contact Center should scan their network and systems at least monthly. All machines with vulnerabilities should at a minimum be updated with patches within 7/30-day patch cycle. Security metrics for systems on the network should be reported quarterly (refer Appendix C) to the IDEA Information Security Team. This is applicable to all Systems, OS and Applications running on the network supporting ICL Business

5.3.9 Network ownership for reporting and incident response should be assigned to the sponsoring ICL business in the ICL *Subnet Inventory*. The ICL *Suspect List* should be regularly monitored by the Trusted Contact Center and suspects investigated and closed within a 48-hour

timeframe.

5.3.10 Modem access (dial-up or ISDN) to the Trusted Contact Center Network is prohibited.

5.4 Activity and Fault Logs

5.4.1 Success and failure for all user account logins, system logins, and administrative requests must be logged for a period of 6 months.

5.4.2 General server event logs, utilization logs, and application events and errors must be periodically verified as functioning in case of a forensics investigation.

5.4.3 The Contact Center must maintain record for all hardware problems and operating system crashes.

5.4.4 Authentication failures and successes must be reviewed (at least weekly) for security violations and need to be stored for 6 months

5.5 Access Controls and Privilege Management

5.5.1 All ICL Data must be protected via access controls. The information must be protected from improper access, disclosure, modification and deletion. See ICL *Data Classification Guidelines*.

5.5.2 ICL data must not be disclosed to unauthorized personnel. Access to ICL data must be approved on a business need basis. Access to servers must be restricted to authorized staff based on function

5.5.3 The users must be given access privileges with the minimum requirements as per their job requirements. Non-administrative users must not have access to administrative system, software or utilities. Privileged or administrative accounts must only be given to the persons responsible for managing systems, databases and applications. Details of people with privilege access should be recorded and stored.

5.5.4 Ensure procedures are in place to add, remove, and modify user access, including details on control of user administration rights.

5.6 User Accounts

5.6.1 General user account requirements

5.6.1.1 Every user must have a unique user ID and the details of the user should be maintained by the administrator SPOC. No shared accounts must be used beyond built-in and system accounts where individual usage can be tracked.

5.6.1.2 The Contact Center security SPOC shall maintain a list of all users ID's used by the Contact Center in the organization and shall provide this list to the IDEA SPOC on a monthly basis.

5.6.1.3 The account owner is responsible for protecting data and resources that are proprietary to

ICL, respecting privacy considerations where appropriate, operating ethically, and following security and legal procedures.

5.6.1.4 Account settings should be configured such that files owned by that account are not world-accessible or other-accessible (for reading, write, or executing) by default. The account owner can modify accessibility as needed.

5.6.1.5 Upon employment termination, all accounts belonging to exiting ICL Workers must be disabled or deleted on their departure date.

5.6.1.6 On a monthly basis all user accounts must be reconciled. Any account that is not owned must be removed. Any account that is not sponsored, is not valid, or has not been accessed during the prior 90 calendar days or longer must be disabled as a secondary control

5.6.1.7 An ICL employee should sponsor all accounts on ICL-managed systems assigned to Contact Center ICL Workers

5.6.1.8 The full name of the ICL employee sponsoring the account should be included in the account profile in readable form such that the account can be easily identified as the responsibility of that employee.

5.6.1.9 When a Contact Center ICL Worker leaves or is no longer actively engaged on a ICL project, it is the responsibility of Contact Center to inform the ICL Sponsor to initiate account termination activities.

5.6.1.10 Disabled accounts to IDEA applications or infrastructure must not be re-enabled until sponsored by a ICL employee and approved by the IDEA IT security team.

5.6.1.11 All Contact Center user account should have an expiry period and need to validate before extending

5.7 Password Policy

5.7.1 Contact Center account access must match or exceed ICL or industry standard password management, and include audits for:

5.7.1.1 Minimum password length and complexity (example: 8 character length, should contain alphanumeric, special character, Uppercase and does not contain your username / Account name).

5.7.1.2 Password change every 45 days

5.7.1.3 Password Reuse: Unique passwords must be selected without reusing any of the previous 4 passwords.

5.7.1.4 Consecutive Login Failures: To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After five (5) unsuccessful attempts to enter a password the account should be lockout. User can

request the system administrator or help desk through proper ticketing methods and approvals to unlock the account if he has forgotten his password and has incidentally lockout his account while guessing the password. Multiple login failure should be logged and reviewed

5.7.1.5 Minimum Password Age: Passwords changed cannot be changed immediately and will need to wait for a minimum period of 1 day to change their password.

5.7.1.6 Session Timeout: Session time-out time should be set after a defined period of inactivity

5.7.1.7 All users will have a unique user ID. Required encryption for sensitive information during network transmission. Two-factor authentication is preferred and may be required for some applications such as remote access (example: RSA SecurID token).

5.7.1.8 All user ID should map to an individual and his up to details has to be maintained by the system administrator

5.7.1.9 If the sponsor of the account is no longer with the organization, user ID's need to re-validated and re assigned to the new sponsor

5.7.2 When an administrator assigns a temporary password to an account, the user should be forced to change the password at the first sign-on.

6 Network Connectivity Security Requirements

6.1 Contact Center Connectivity

6.1.1 Based upon ICL business access type and security requirements established ensure the Network Connectivity Security Requirements to assess access security controls are audited.

6.1.2 Each Contact Center Connection should have a termination date that is not more than 18 months from the start of the connection. The ICL Sponsor is responsible for reviewing and either renewing or terminating the connection prior to the termination date. If the connection needs to continue after the termination date, a review of the connection should take place to ensure the correct security measures are in place to meet any new or updated business needs and to utilize new technology. This review should take place prior to the termination date to ensure continued service.

6.2 Contact Center Network Transport Requirements

6.2.1 Access to the Network of IDEA is allowed through secure channels (like MPLS, VPN, IPSEC, SSL, etc..) only. Any remote access should be accompanied by AAA protocols (Authentication, authorization, access control). All applicable TRAI Security mandate has to be followed for any remote access

6.2.2 A site-to-site connection between the Contact Center network and ICL internal network should have a firewall with logging enabled

6.2.2.1 The ICL firewall should be on the ICL network in an ICL-controlled facility.

6.2.2.2 The interface between the Contact Center and ICL should be monitored for inappropriate activity using Antivirus, intrusion detection or preferably prevention systems (NIDS/NIPS) or monitored firewall IDS/IPS. Any abnormal events should be bought to the notice of ICL security team

6.2.2.3 It is recommended that the Contact Center protect its internal network from ICL by implementing a Third Party-managed firewall with Least Access rules. Any incident or abnormal events noticed, should be escalated to ICL Security team immediately

6.2.3 Access to and from ICL to the Contact Center network should be reviewed and approved by the IDEA Information Security Team

6.2.3.1 Rules should specify IP-to-IP access with specific ports and protocols.

6.2.3.2 Contact Center and ICL should not use NetBIOS protocols (for example 135/137/138/139/445). Any exceptions should have IDEA security Team's approval

6.2.3.3 ICL should not allow Basic Contact Center access to corporate shared resources such as internal instant messaging, email, DNS, and shared web portals. However they may use our

NTP server to ensure time stamps are synced across systems.

6.2.3.4 For inbound access to ICL, if a large network range (DHCP), or the protocol used does not support authentication, or it allows general next hop access (telnet/SSH), then the approval should require authentication of the Contact Center prior to ICL network access. Methods include two-factor logged/control Citrix access, Nortel IPSec, SSL-VPN, or ICL network proxy with restricted access.

6.2.4 A site-to-site connection between Contact Center network and ICL internal network requires NAT of ICL internal addresses.

6.2.5 Physical Security—access restricted to Contact Center ICL Workers assigned to ICL contracts and briefed on ICL acceptable use policies.

6.3 Trusted Contact Center Outbound Proxy Servers

6.3.1 ICL recommends blocking Anonymizers/Translators, Sex, Drugs, Hate Speech, Criminal Skills, Gambling, Games, Extreme/Obscene/Violence, Chat, Webmail, Dating, and Cults/Occult. All access which could lead to information security and data leakage threat should be blocked / controlled

6.3.2 Logs of proxy should periodically be reviewed for potential violations.

6.3.3 Internet access for Contact Center dedicatedly supporting ICL should be limited to business purpose. Controls should be in place in alignment with ICL Internet access policy or higher

6.4 Trusted Contact Center Email Servers

6.4.1 Block the following attachment types in email, with periodic updates by the IDEA Information Security Team. Restrictions have been placed on the types of email file attachments that should be permitted when communicating with ICL and its customers. The restrictions apply to incoming and outgoing messages, both internal to ICL and to/from external addresses. Attachments of most of the common file types are permitted. These include: Word (.doc), Excel (.xls), PowerPoint (.ppt), Images (e.g., .jpg) and PKZIP (.zip). HTTP links embedded in the email pointing to internal or external web addresses are also permitted.

6.4.1.1 Contact Center should block following file extensions like ade;adp;app;asf;asx;bas;bat; bz2;chm;cmd;cnt;com;cpl;crt;dll;eml;exe;fxp;hlp;hta;inf;ins;isp;js;jse;lnk;mdb;mde;mht ;msc;msi;msp;mst;pcd;pif;prg;rar;reg;scr;sct;shb;shs;url;vb;vbe;vbs;wmd;wsf;wsc;wsh. All inbound and outbound emails should be scanned using latest antivirus signatures

6.4.2 ICL shared service email servers are preferred for ICL Confidential/Restricted business processes. .

6.4.3 Access to personal Emails should not be allowed considering the potential of data leakage and virus infections

For all communication to ICL Information Security team : information.security@idea.adityabirla.com

7 Appendix

7.1 Appendix A: ICL Data Classification Guidelines

third party data classification guideline

7.2 Appendix B: ICL Acceptable Use Guidelines

Idea Acceptable Usage Policy Agreem

7.3 Appendix C: ICL Contact Center Metrics

ICL Contact Center - Metrics.xls

7.4 Appendix D: ICL Contact Center - Risk Register Template

ICL Contact Center - Risk Register Templat