Excellence in Legal Practice

ICT POLICY

FOREWORD

Information and communication technology (ICT) is the central engine that is driving economic transformation of Rwanda. In this regards, the Institute of Legal Practice and Development (ILPD) has and is still investing in ICT infrastructure development to professionalize its services and get benefits from that enabler.

To get the benefits expected from the investment made in ICT infrastructure, the administration of the Institute has thought to develop an ICT policy, which shall guide further infrastructure development in this domain, and help different users of such a tool in a professional and ethical manner.

The ICT Policy sets key rules and regulations that Institute's users should observe and maintain. We are convinced that the list of do's don'ts in this policy is not exhaustive and will never be, but simply serve to guide. Therefore, the ICT policy is there to add on moral values and conduct of users of the Institute's ICT infrastructure and equipment.

The main objective of this ICT Policy is to create a secure environment of electronic computing communication and encourage ILPD staff and trainees to use ICT infrastructure, equipment and resources responsibly. We believe that our compliance with the policy shall help us to benefit more from the investment made in the domain of ICT.

Table of Contents

Glossary

Ergonomic	Designing or arranging workplaces, products and systems so that they fit the people who use them.
Disaster recovery	The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
ICT Risk	The potential that a given threat will explore vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
Encryption	Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Encryption prevents any non-authorized party from reading or changing data.
Enterprise Architecture	A set of technical guidelines and standards to guide the enterprise in satisfying business needs. It comprises preferred technologies and vendors, templates, tools, methods and standards.
GoR	Government of Rwanda
Institute	Institute of Legal Practice and Development (ILPD)
Risk Log	Details all identified **risks**, including description, category, cause, probability of occurring, impact on objectives, proposed responses, owners, and current **status**
WPA2	Wi-Fi Protected Access II is security protocol and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

PART ONE: GENERAL

1. Introduction

Information Communication Technology (ICT) infrastructure of the Institute of Legal Practice and Development (ILPD) plays an important role in the implementation of the Institute's mission. The budget allocated to the strengthening of ICT infrastructure is huge, and this is a continuous activity. Considering the paramount role of ICT infrastructure and equipment in the daily life of the Institute and given the huge number of users of this equipment, a need to develop a policy in matters of ICT was found imminent.

The intent of this policy document is to provide broad guidelines on the use of ICT equipment and tools of the Institute. This Policy is expected to boost the use of ICT in teaching, learning, and other support activities of the Institute while complying with rules and regulations that ensure return on investment as well as maintaining of discipline.

2. ICT Situational Analysis at ILPD

The Institute of Legal Practice and Development accomplished many ICT projects that support academic and administrative functions. The projects completed include establishment and enhancement of Local Area Network (LAN) both at its headquarters in Nyanza District and in the Kigali Liaison Office; equipping of computer laboratories; designing and maintenance of the Institute's website; computerization of library services; expansion of wireless internet to cover all the ILPD premises of Nyanza; a mega project of Management Information System, just to mention a few.

IFMIS, RBM and smart IPPIS, Online declaration of RRA, E-procurement, Internet banking system and E-procurement help to offer and access related services online.

Another area of enhancement of ICT use at the ILPD includes growing ICT literacy in the community of the Institute. This initiative has been inspired by the National ICT policy and the Justice Sector ICT policy coupled with the strong will of the Institute's administration to embrace and prioritize the strengthening of ICT infrastructure and the use of ICT in delivery of all services where possible.

Though so far the Institute has done a lot in terms of setting up ICT infrastructure, it is still facing challenges. These include unstable electricity, inadequate ICT security systems, inadequate local content on the Web and high cost of subscription to the needed bandwidth as well as hosting its MIS, and inadequate number of staff with the required IT professional skills. Other challenges include increasingly-sophisticated ICT-related security risks, threats and attacks, and the rapid developments in this domain.

3. Purpose of the ICT policy

The purpose of this policy is to clearly define the processes and procedures that shall ensure the effective management of ICT infrastructure as well as equipment within the Institute and obtaining value from them. Specifically, the policy aims to:

i. Ensure that ICT-implemented services are aligned with the institute needs and objectives;
ii. Improve the utilization of ICT resources;
iii. Provide services that meet the institute's business, stakeholder and users' needs;
iv. Improve risk management and resilience;
v. Make staff aware of their roles and responsibilities regarding the use of ICT (dos and don'ts of using ICT resources);
vi. Prevent any usage that could damage the image of the Institute, threaten security of the computer networks, Institute's ICT infrastructure and equipment, or protect any information that may expose ILPD to risk of litigation due to staff or student misconduct;
vii. Prevent misuse of institute's ICT resources;
viii. Ensure compliance with all Government standards related to ICT services management practices as mandated by Rwanda Information Society Authority.

4. Scope

This policy applies to all departments and units of the Institute and is issued by the Management of the Institute. The policy shall be managed by the Information and Communication Technology section of the Institute. This policy applies to users while using

any computing facilities of the Institute at any of its premises but also users using their devices but connected to the Institute's networks.

PART TWO: POLICY STATEMENTS

5.1 Obligations of ICT users

While using the Institute's ICT equipment or connecting to its network, the users must adhere to the following:

- Exercise professionalism by respecting the integrity and reputation of the Institute;
- Comply with all rules and regulations listed in this policy;
- Be accountable for their activities done using IT equipment or ICT infrastructure of the Institute;
- Report any technical issue to the ICT section of the Institute;
- Ensure that any use of the above described ICT infrastructure or network is meant for professional reasons.

5.2 Project Management

All major ICT projects of the Institute must follow a formal project management methodology. This methodology must, at a minimum, stipulate the following project deliverables within the respective phases of the project:

a. Project Initiation – Project charter.

b. Project Definition – Project definition report, Project plan and Business justification.

c. Execution – Project status reports.

d. Close out – Project completion report.

e. Maintenance

Each project designed for ILPD must be fully documented, and the documentation must include a manual and an administration training manual.

5.3 Risk Management

Though a significant part of ICT is very useful and an enabler to effective and efficient work, there are some risks associated with its use. There must thus be strategies to mitigate against

those risks and where possible avoid them. The following must be done for ICT risk management:

- An ICT risk data bank for the Institute must be developed and ranked;
- The risk management process must be followed and must be aligned to the RISA risk Management Guidelines;
- Any ICT equipment whose value is more than two million Rwandan Francs must be insured;
- A risk log must be maintained for the most significant ICT risk issues identified and these issues must be monitored regularly and dealt with.

5.4 Information retention and disposal

Information must be retained and disposed of in line with statutory and Institute requirements. Failure to comply with statutory and Institute requirements could result in a financial loss, legal actions, and embarrassment to the Institute, unavailability of needed information and wastage of resources in managing obsolete information. Therefore, before disposing of an ICT equipment that stores the Institute's information, the following steps must be complied with:

- Diagnosis of the information stored on the device;
- Identifying information resource that should be retained, and the most cost-effective means of retention;
- Storing of information on storage media that is the most cost-effective and meets requirements;
- Ensuring that when highly confidential and restricted information is destroyed, its confidentiality is not compromised;
- Ensuring that information that is classified as highly confidential or restricted has appropriate levels of access control;
- Indexing all information stored on the Institute's repository to facilitate easy identification, retrieval, and destruction at the end of its retention period;
- Destroying information that falls outside of retention periods specified by the Institute or that is obsolete and no longer has any value to the Institute.

5.5 ICT Asset retention

To avoid deterioration in the productivity of the Institute's ICT assets, coupled with high maintenance cost, a minimum lifespan is allocated to the different categories of these assets:

Description of Asset	Expected Lifespan
Desktop Personnel Computer, Audio equipment, monitor, and Television screen, tablets	5 Years
Laptop and Tablet	2 Years
Printers, Scanners, Photocopying machine and projectors	5 Years
Servers, Storage devices (NAS, external hard disk)	5 Years
Desktop software, operating systems	5 years
ICT toolkit	3 Years
Network switch, Access point and WIFI antenna	5 years

It must be noted that the mentioned lifetime stated above is the minimum life time expected for a new acquired asset. At the end of the expected lifetime of each asset, a decision to retire the asset should be reviewed in terms of the residual business value and cost of maintenance.

A retired asset must be erased of any data, information and software by partitioning the relevant hard drives. After consultation with competent organs, the Institute may decide to donate retired assets, as a support, to schools, organizations or associations of non-profit. Alternatively, the Institute may sell those ICT retired assets through E-auction. Damaged or completely ruined ICT assets should be given to the government authority in charge of disposing off ICT equipment. In any of the cases, IT equipment must be erased of any data, information and software by partitioning the relevant hard drives, before leaving the Institute store.

5.6 Acquisition of ICT equipment and Software

To assure that acquired ICT equipment match with real needs of the Institute and maximize the value for money, the following steps must be taken in the process of acquisition:

- A thorough investigation on the equipment or service to be acquired. There must be a valid business requirement with a formal definition of information requirements that is agreed between the user and ICT section and auditable;
- All IT purchases must be conducted in accordance with public procurement rules and regulations;
- For acquisition of a computerized solution, a technological feasibility study must be conducted to ensure that the proposed ICT solutions shall be compatible with existing ICT architecture.
- ICT security and risk considerations must be built into the ICT architectural criteria;
- An economic feasibility study entailing a cost-benefit analysis must be conducted to establish the availability of enough funds to implement the preferred alternative solution;
- Ergonomic or comfort design factors must be taken into consideration and must be in line with regulatory requirements;
- When selecting ICT solutions, the software licensing requirements must always be adhered to, to ensure that the Institute is in no way exposed to liability in terms of illegal software;
- For computer solutions, a contract of acquisition must include maintenance phase to ensure that software updates shall be available within the agreed timeframe in case of bugs fixing or changes required;
- A checklist report of the fulfillment of the above-mentioned conditions and criteria of selection of a vender must be produced by ICT section;
- In a case of new or modified computing facility (ies), a formal acceptance of facility (ies) must be signed by the Institute appointed project manager, stating that the facilities are in compliance with specifications.

5.7 Applications Development

All applications development must follow a defined software development lifecycle (SDLC) by going through the following steps:

- Input requirements definition and documentation;
- Interface definition;
- Source data collection design;
- Programme specification;
- File requirements definition and documentation;

- Processing requirements;
- Output requirements definition;
- Internal controls;
- Auditability;
- Security and availability;
- Testing requirements.

Each application designed for ILPD must be fully documented. The documentation has to include a well prepared user manual, administration training manual and application source code.

5.8 Software Licensing

Software systems or applications installed on the Institute's devices must adhere to regulations and requirements of their developers. Only genuine software applications or systems are allowed on the Institute's devices. Therefore, the following must be strictly respected before installing or using any applications/systems on the Institute's devices:

- Only software for which a legal contract exists should be installed on ICT assets of the Institute;
- Installation of software/system must be done by the Institute's IT Professionals or with their assistance;
- When a software contract expires and is not to be renewed, the software must be uninstalled from Institute's assets;
- Licensed software or related documentation should not be duplicated for use either on the Institute premises or elsewhere unless the Institute is expressly authorized to do so by agreement with the licensor, and this has to be approved by the relevant ICT manager;
- CD's containing software may not be loaned to any users or contractors unless expressly authorized to do so by agreement with the licensor, and this to be approved by the relevant ICT manager;
- Software on multiple machines may only be installed in accordance with the applicable license agreements;
- No Shareware or Freeware should be loaded onto Institute ICT assets without the written permission of the ICT manager.

5.9 Change Control

- All changes to the IT environment must follow a formal change management process that ensures that all changes requests to applications, procedures, processes and platforms are handled in a standardized manner;
- All requests for change must be assessed in a structured manner for all possible impacts to the overall ICT environment;
- Changes must be categorized and prioritized so that urgent changes follow separate formal procedures;
- Changes must follow a defined change approval process with defined authorities in the change management process;
- A register of changes must be maintained for all changes to the ICT resources.

5.10 IT Asset Management

Institute ICT assets must be managed across their full lifecycle encompassing acquisition, redeployment, storage and disposal. An inventory of institute ICT hardware assets such as servers, workstations, laptops, tablets, modems, switches, routers, firewalls, printers etc must be maintained and kept up-to-date.

An initial baseline must be recognized containing all institute ICT assets and compared regularly against a physical inventory of institute ICT assets to identify changes. Any ICT asset should be handed over to the logistics officer when the user no longer uses it or is no longer employee of the Institute.

5.11 Logical Security

- Unique user identification and authentication systems must be applied to prevent unauthorized access to internal resources e.g. passwords, pins, and token devices.
- User account management must be enforced, and a formal process must be followed for requesting, approving, establishing, issuing, suspending, modifying and closing user accounts.
- Access privileges must only be granted on a need to use basis and in accordance with the relevant user's requirements necessary to carry out their job function.

- All connections to the Internet or other public networks must be protected by firewalls configured to filter traffic and ensure against denial of service attacks and unauthorized access to internal resources.

- Data encryption facilities must be utilized in accordance with the GoR's Information Classification Scheme.

5.11 Physical Security

- The location of computer facilities rooms must be protected sufficiently, and must be sited away from areas of public access;
- The institute should have appropriate fire extinguishers to serve in case of a fire incident;
- No resources within computer facilities rooms should be visible externally;
- Wiring closets must be physically secure with only authorized access possible and the cabling routed as much as possible underground or through secured conduits;
- Doors, windows, elevators, docking stations, air vents and ducts and other methods of access to the computer facilities rooms must be adequately secured;
- An appropriate alarm system must be installed in the computer facilities rooms to detect and warn people through visual and audio appliances when smoke, fire carbon monoxide or other emergencies are present;
- Access to computer facilities rooms must be well controlled by possible user card readers or another adequate security system;
- Visitors to computer facilities rooms e.g. cleaning staff and third parties must be escorted and reasons for entry must be logged.

5.12 Credentials Management

All Institute's applications, whether developed internally or by partners/stakeholders shall be accessed using credentials (*user name and password*) allocated to each user. Such credentials should be properly managed and kept in secrecy. Users of systems and applications should adhere to the following:

- Not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical user accounts shall be maintained securely;
- Change of passwords whenever there is any indication/suspicion of possible system or password compromise;
- Change Passwords at regular intervals of 90 days or less. Based on the number of access, passwords for privileged accounts should be changed more frequently than normal accounts, and avoid reusing or cycling old passwords;

- change temporary passwords at first logon;
- Do not include password in any automated logon process, e.g.: stored in a macro or function key;
- Do not share passwords with anyone else;
- Never use a password at the watch of anyone else.

For security purposes, a password should be:

i.Unique.
ii. Alphanumeric.
iii. At least 10 characters in length.
iv. Regularly changed.

5.13 Environmental Control

- The ICT staff must take reasonable steps to protect all ICT hardware from natural and man-made disasters. The device for control of network of the Institute must be hosted in server rooms or lockable cabinets. Server rooms must always be of solid construction and locked;
- A maintenance schedule must be established and maintained for all ICT hardware of the Institute, and they must be recorded in a maintenance register;
- Hazardous or flammable materials must not be stored in the computer facilities rooms or near any other critical information processing device;
- Eating, drinking or smoking inside the computer facilities rooms is strictly prohibited;
- Dust covers must be used to protect critical information processing equipment;
- Human-friendly fire prevention and detection systems must be installed in the computer facilities rooms and must be regularly tested;
- No unsafe electrical wiring or cluttered areas are allowed within the computer facilities rooms;
- Power protection controls must be installed to prevent power outages or surges e.g. uninterrupted power supply systems, lighting conductors and backup generators;
- Air conditioning, ventilation and humidity controls must be installed and kept at optimum levels;
- Enough drainage must be employed in computer facilities rooms to prevent flooding;
- Safety and health measures must be implemented in computer facilities rooms e.g. having clearly marked escape routes and first aid kits;

- The off-site location, used to store backup data media, must be protected with the following physical security measures: Having a building of solid construction, physical access control, installing and putting in place fire detection and suppression equipment.

5.14 Network Security and Wireless Networks

The network structure and configuration including IP addresses, location, and model of all switches, routers and firewalls must be documented, and the Firewall must be installed between network and public network to block intrusion attempts. The security software should be used to scan the entire network monthly to detect security vulnerabilities. The scans must be performed from the Internet, as well as from the internal network.

The Institute's wireless networks must be configured within the following standards:

i. *WPA2 security protocol or better;*

ii. *Password strength of at least 10 characters with a combination of alphanumeric characters and symbols.*

iii. *Latest firmware installed, and*

iv. *Default system usernames and passwords must be removed.*

5.15 Business Continuity and Disaster Recovery

A Business continuity and disaster recovery plan must be established, maintained and periodically tested for all critical information resources. The disaster recovery plan must define:

i. *Procedures for assessing damage, escalation procedures and declaring a disaster;*

ii. *Roles and responsibilities of disaster recovery team members, including third parties, their contact details and communication procedures. Prioritized recovery procedures based on the criticality of information resources;*

iii. *Backup procedures, manual procedures, alternative processing facilities and safety, and health procedures.*

The ICT Disaster Recovery plan must be stored in hard and soft copy in a safe place and should be accessible in the event of network failure. The ICT Disaster Recovery plan must be securely distributed and available only to authorized personnel.

Essential hot spares (Backup component) must be stored and be easily retrievable in the event of a disaster.

Reciprocal agreements must be entered into with all parties involved in the disaster recovery process.

Disaster recovery training sessions must be undertaken by the team in charge to ensure its preparedness in case of a disaster.

5.16 Performance and Capacity Management

- Daily health checks must be conducted on critical ICT resources. The checks must include, amongst others disk capacity, network bandwidth, buffer sizes, database size, error logs, consumables e.g. printer toner, printer paper, WAN and LAN connectivity checks;
- Performance reporting must occur on all critical ICT resources on a regular basis;
- Performance requirements must be included as part of every new application development, implementation or modification project;
- Capacity planning reviews must be conducted regularly to forecast future ICT requirements.

5.17 Data Management

Procedures must be implemented to prevent access to sensitive data and software from equipment or media when they are disposed of or used for another purpose e.g. partitioning of hard drives. Storage and retention arrangements for data must be in accordance with legal, regulatory and business requirements. Backups must be performed based on a defined cycle and must include, at a minimum critical databases' master files and transaction files, critical applications, configuration settings and user documentation.

Backup media must be clearly labelled, prevented from overwriting, appropriately stored and protected in transit e.g. in secure containers.

Backup of sensitive data must be protected in accordance with the GoR Information classification scheme e.g. encrypted when necessary. Backups must be checked periodically to determine whether recovery is possible.

5.18 Email Usage

ILPD has email server where each staff of the Institute must have an official email. Users of the Institute's email server must adhere to the following:

- only use the Institute email (@ilpd.ac.rw) for official communication whether internal or external;
- Use email as a business communication tool and be responsible for contents of their messages;
- Archive their emails on regular intervals;
- Protect access to their email accounts through strong passwords and never share their passwords or accounts with anyone else;
- promptly report to ICT officer(s) all suspected security vulnerabilities ;
- Avoid opening mail from unknown sources, suspicious attachments or clicking on suspicious links;
- avoid sending or forwarding unsolicited email messages, chain letters, Jocks, junk mail, etc…. from other internal users and external networks or other advertising material to individuals who did not specifically request such material (email spam);
- Avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

5.19 Internet Usage

The Internet is a very crucial facility in the current era. It is used in the work environment, in teaching, learning and research. The Internet is a very power facility such that the world would not be as it is today without it. However, as much as the Internet is so useful in simplifying work, it may well be utilised to do wrong things. Therefore, users of the Internet of the Institute must avoid the following:

- Use another person's username and password at any time to access the network or email;
- Allow someone else to access one's account on network or systems;
- Access another person's files or data without permission;
- Use computer programs to decode passwords or access control information unless authorized by the administration of the Institute;
- Attempt to circumvent or subvert system security measures;
- Engage in any activity that might be harmful to computers or to any information stored in them, such as creating or propagating viruses, disrupting services, or damaging files;
- Use the Institute's systems for partisan political purposes such as using electronic mail to circulate political agenda, do political campaigns etc;

- Transmit spam, junk mail, chain letters, pyramid schemes, or the like using or through the Institute's systems or networks;
- Use the Institute's systems or networks to transmit content that is obscene, defamatory, libelous, slanderous, threatening, harassing, abusive, hateful, or racially or ethnically offensive to any other person, or that is unlawful or encourages conduct that would be considered a criminal offense, give rise to civil liability or violate any law;
- Use the Institute's systems or networks to stalk or impersonate any person;
- Make or use illegal copies of copyrighted software or information, store such items on the Institute's systems, or transmit them over the Institute networks;
- Use Institute resources to harass, intimidate, or otherwise annoy another person, for example by broadcasting unsolicited messages or sending unwanted mail;
- Use the Institute's systems or networks to create personal web pages containing pornography, abusive words or profane language;
- Use the Institute's network to access or view pornographic material;
- Modify or abuse computing resources, for example, by intentionally placing a program in an endless loop;
- Use the Institute's systems or network for personal gain, for example, by selling access to internet, use of computer or other devices or by performing work for profit in a manner not authorized by the Institute;
- Engage in any other activity that does not comply with the General Principles presented above.

5. 20 Security Incident Management

All users who are given access to Institute information, IT and communications facilities have the responsibility to:

- Minimize the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it;
- Report suspected information security incidents promptly so that appropriate action can be taken to minimize harm;
- Report the loss or theft of electronic records, or IT equipment such as tablets, laptops and smartphones or other devices on which data is stored;
- Report any Denial-of-Service or other cyber-attack on IT systems or networks;

- Report the power outage that affects access to IT systems and information services;
- Report any breaches of physical security e.g. forcing of doors or windows into secure room.

PART THREE: PAPERLESS IMPLEMENTATION

6. Rationale

The huge investment the Institute makes in ICT infrastructure development aims at digitizing its services such that they can be offered online, and progressively bring the use of papers to an end. Gone are the days where an employee could be expected to work only when he or she is in office. For any institution to remain relevant in today's competitive market it must cope with the trend of potential beneficiaries of its services and stakeholders who wish to get responses to their demands without leaving their stations.

Therefore, to cope with such demand for online services, investment in ICT infrastructure alone cannot suffice but also having staff ready and equipped to offer those services is essential. In this regard, it has been observed that it would be more convenient and productive if staff of the Institute would have portable computers such that they can work or offer services even outside offices when needed. However, staff could not be required to bear the cost of purchasing laptops yet it is an obligation of the employer to avail office space and equipment to the employee. It was therefore decided to facilitate staff members to have laptops to use for official work which can be done both in office or even outside office.

7. Facilitation

The Institute resolved to facilitate its employee to get portable computers which enable them to render services even outside its (the Institute's) premises. Facilitation for staff to have laptops, which are to replace computer desktops, shall be done through co-ownership agreements between the Institute and each staff member.

8. Laptop Co-ownership Agreement

8.1 An agreement for co-ownership shall be signed between a staff member, who receives a brand new computer laptop, and the Institute.

8.2 The Institute shall acquire laptops of good quality every year and distribute them to staff starting from those who are custodian of services that are demanded online.

8.3 Staff members shall be required to reimburse half of the cost of the laptop in a period not exceeding ten (10) months.

8.4 The period of co-ownership should be two years equivalent to the life time of the laptop.

8.5 After the period of co-ownership, the residual value of the laptop becomes the exclusive property of the staff member who had co-owned it with the Institute. The staff member however, should keep using it for official work of the Institute until he or she becomes again beneficiary of a new scheme.

8.6 The scheme should be applicable to permanent staff, but can also be extended to contractual staff whose contracts are likely to take longer.

PART FOUR: IMPLEMENTATION, REVIEWS AND ENFORCEMENT

9.1 Approval and Amendments Sheet

This policy is approved by: Management of the Institute of Legal Practice and Development (ILPD).

9.2 Review

In order to ensure that the Institute ICT assets are adequately protected and that this policy remains relevant, a review of this policy shall occur once a year.

Records of Amendments

Version no.	Description of Amendment	Date

9.3 Breach of the ILPD's ICT Policy

ILPD staff members and students are expected to report any apparent breach of these guidelines to relevant higher authorities. If any equipment is damaged, lost or stolen while under the care of ILPD staff members or students, its purchase price shall be reimbursed by the responsible person unless it is proved that the loss could not have been avoided. Failure by a

staff member to comply with this policy will be deemed misconduct. Apparent breaches of this policy will be investigated and if confirmed with due proof, it may result in disciplinary action, including dismissal in case of serious or persistent breaches.