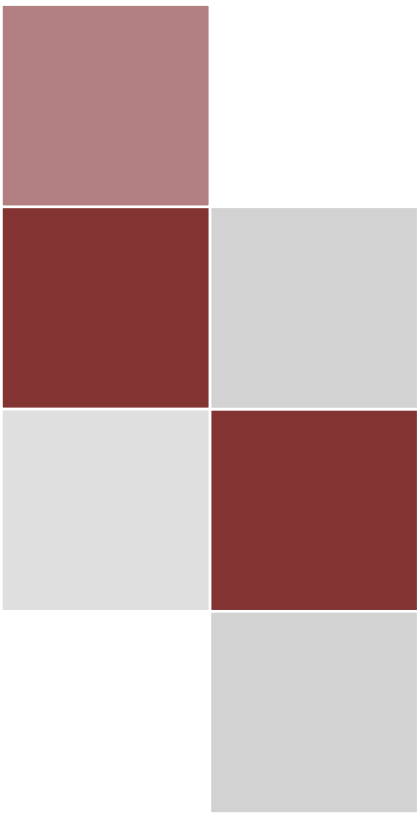
CGIAR

ILRI

INTERNATIONAL LIVESTOCK RESEARCH INSTITUTE



ILRI security policy

October 2013

Contents

POLICY STATEMENT

The International Livestock Research Institute (ILRI) works at the crossroads of livestock and poverty, bringing high-quality livestock science, communications and capacity building to bear on poverty reduction and sustainable development. ILRI has main campuses in Kenya (headquarters) and Ethiopia (principal site), with other offices located in Southern and West Africa, South Asia, Southeast Asia and East Asia. ILRI staff travel extensively and carry out field work/activities in many remote parts of the globe.

ILRI strives to ensure a secure and productive work environment by providing standards of security that are reflective of an international research and development organization. It is in this context that we formulate and enforce our security policy in collaboration with host governments. We view security as a collective responsibility to detect, prevent, pre-empt and deter any threat to our safety and well-being from any individual, group or institution. There is a need for total collaboration by all staff with ILRI internal security services and other security agencies of the host countries. Our policy demands that all ILRI staff, their dependants, visitors and any other ILRI premises users obey and heed any security instructions that may be issued at any time, according to the prevailing security situation. More importantly, all staff members are reminded that immunity is not absolute and they are required to obey and comply with the laws of the host country.

ILRI will endeavour as much as possible to ensure that;

- Staff work and live in a secure environment by coordinating efforts between the Security Unit, private security providers and the host government security agencies
- All staff understand their security responsibility and adhere to personal security standards and advice
- Plans and procedures are developed to guide emergency, evacuation and crisis management responses
- Security instructions are transmitted to staff in a timely and accurate manner
- Staff follow security instructions and positively respond to any changes according to security situation
- Staff assist internal security services as much as possible to detect, prevent, pre-empt and deter criminals or would-be criminals by providing to security personnel any useful information - confidential or otherwise - that could facilitate any internal investigation necessary to establish certain facts
- Security Unit personnel are well equipped to discharge their duties professionally and diligently.

INTRODUCTION

This document contains much of the information that ILRI management and staff need to know about security and their role in ensuring a secure working environment — by helping prevent crime and assisting ILRI security personnel in planning, coordinating and enforcing security structures that exist in and around ILRI. It is therefore the responsibility of each ILRI staff member to read and understand this document.

Risks that ILRI staff and property are exposed to include (but not limited to):

- Criminal
- Biological
- Chemical
- Political
- Natural

Purpose

The purpose of this document is to establish a general policy governing ILRI's security and its management. The document outlines the guidelines, references and implementation procedures that will enhance continuity and consistence in security plans.

Applicability

This policy applies to all ILRI operations, staff and other individuals associated with the work of ILRI.

References

The policy makes reference to other documents also provided separately touching on specific security issues as follows:

- ILRI evacuation plan
  cgspace.cgiar.org/handle/10568/34153
- ILRI crisis management plan
  cgspace.cgiar.org/handle/10568/34150
- ILRI ICT security policies
  ilrinet.ilri.cgiar.org/index.php?option=com_content&view=article&id=163&Itemid=359
- ILRI Travel Security guidelines
  cgspace.cgiar.org/handle/10568/34405

RESPONSIBILITY AND ORGANIZATION

Overall responsibility for security in ILRI is a management function under the leadership of the Director General (DG). Responsibility for the management and implementation of the security plans and directives lies with the Security Unit led by the Chief Security Officer (CSO).

Director General (DG)

- Responsible for providing leadership and the necessary resources to support the overall security plan.
- Serves as the leader of the Crisis Management Team (CMT).

Chief Security Officer (CSO)

Functions as follows:

- Serves as the security coordinator and chief warden.
- Performs security risk surveys, assessments and recommends mitigating actions for all aspects of ILRI security operations.
- Liaison with security agencies, companies, embassies, local authorities, clients and subcontractors on matters specific to security.
- Ensures provision of physical security, guards and enhances the supervision of the same.
- Manages the relationship with the out-sourced service providers for security guards, intruder alarms systems, CCTV and access control systems.
- Formulates and implements security standard operating procedures in conjunction with ILRI management.
- Manages emergency and operational security communications networks.
- Coordinates emergency response and assistance to staff.
- Oversees the overall operational and day to day function of the Security Unit.
- Responsible for developing and maintaining programs to assess security and well - being of all personnel working for ILRI.
- Ensures the design, review and rehearsal of contingency plans for crisis response, security, evacuation and medical-related incidents.
- Coordinates information on local security situations and disseminates the information to staff when appropriate and other individuals associated with the work of ILRI.

THREAT ASSESSMENT PROCEDURES

Risk Analysis

In order to ensure that appropriate security measures are maintained, security analyses/assessments will be conducted and the CSO will maintain a record of each security analysis on file. The security analysis will be based on a risk assessment, which will consider:

- Threats to ILRI campuses
- Threats to regional offices
- Risk levels of these threats
- Potential impact on research and operations
- Manageability and mitigation of the risks

In order to identify the threats and determine the risk levels, security information networks will be developed to gain accurate and timely information. In so doing, regional representatives will monitor real time security and safety risks to the establishment as opposed to speculation. They will gain real time information on specific threats, which may be crucial to research activities. Sources will include but not limited to:

- Police
- ILRI Security Unit
- Other CG Center's Security Units
- US State Department Public Awareness Announcements
- Embassy and High Commission briefings
- Third party security groups such as Frontier MEDEX, Control Risk Group, UN Inter Agency Working Group on Security
- UN security updates and briefings
- Private Security Providers
- Local knowledge
- Media
- Other security operatives
- Trade/business forums
- Contacts in government/military/law enforcement/intelligence

Overview of the Security Situation

The risk assessments will first consider ILRI operations as a whole. ILRI's regional/country locations may be then assessed individually and/or divided into zones to assist in determining location specific levels of risk. Severity of risk will be expressed in terms of:

- Insignificant
- Low
- Medium
- High
- Extreme

This part of the risk assessment will include a summary of the main threats and likely future threats.

Threats to ILRI

Risk assessments will consider recent security incidents and security information in detail and will identify specific threats to research operations and will consider how best to manage such risks. Results of the risk assessment will lead to the design and implementation of appropriate security measures.

Security Advisories

The Security Unit will publish security advisories to all ILRI staff to update on any changes in the security situation within the areas of operation and will also highlight security emergency issues that may directly affect staff. Only the Security Unit will have the authority to broadcast security advisories to staff.

SECURITY FORCES

It is the overall responsibility of the host government to protect ILRI staff and property. However, the need for an exercise of force against a threat must be first evaluated by an appropriate ILRI official and only implemented by government security agencies after a formal request for assistance is issued – usually limited to cases involving extreme and immediate danger. If the situation so warrants, only after consultation with ILRI DG or his/her designate and in adherence to ILRI's host country agreement, shall government forces be permitted to enter ILRI premises.

Internally, the responsibility to protect staff and property of ILRI is under the authority of the ILRI DG. However, if physical threats exist beyond the capacity of in-house ILRI security, ILRI will call for the assistance of the government security forces. On calling for assistance, ILRI will make every effort where possible to ensure:

- Staff, their dependants, visitors and contractors on ILRI premises are kept informed of developments.
- The situation is resolved with minimum force.
- Security force operations are conducted within the rule of law.
- Human rights are not abused.

Close liaison with senior government officials will potentially help ensure that government security forces deployed to ILRI facilities maintain the highest professional law enforcement standards.

TRAVEL SECURITY

Field Work and Travel Restrictions

Before proceeding to the field for field work, staff will have to fill in a Field Risk Assessment Form. This form will be checked and verified by the CSO and the EOHS Manager before the relevant Supervisor or Director can approve.

Where ILRI operates in high-risk areas, Directors, through security updates and advisories, will determine areas which are out of bounds or where special measures may be required.

Travel Information and Communication

Prior to departure to any long travel destination, either internationally or locally especially if heading to an unfamiliar environment, staff are advised to visit the following websites for information prior to departure.

www.fco.gov.uk/travel
http://travel.state.gov/travel/
www.frontiermedex.com

Communications with Head Office, Regional Offices, Security Units, Supervisors and others while in the field or on mission travel will be done using the traditional means. These are phone [landline or mobile], fax, email, skype, text etc. Where it has been determined beforehand that communication will be a challenge, the use of satellite phones is encouraged. These are available from the Security Units in Nairobi and Addis and from the Regional Reps in the regions.

- Always visit the above websites before departure
- Ensure you have all contact details of your host at your final destination
- For more information, please refer to the ILRI Travel Security Guidelines http://ilrinet.ilri.cgiar.org/Datafiles/files/FinanceOperations/Security/ILRI_Travel_Security.pdf
- Always have coloured copies of your passport bio data pages in your possession and on your person
- Unless necessary, do not move around with your passport and other valuables. Have these secured in a safe place

High Value Goods

Where possible, the movement of high value goods will be carried out by suppliers or contractors. Where this is not possible, a risk assessment will be made by management, balancing the need for protection against the need for a low profile. Insurance of goods will be considered as a part of this assessment.

Vehicles Management

All vehicle usage will be recorded in a logbook. Drivers will report on departure and arrival and at pre-determined intervals. If a driver fails to report back, security staff will be alerted and search procedures will be implemented if necessary.

COMMUNITY RELATIONS

While the major responsibility for community development rests with the host government ILRI recognizes the need to engage with communities in order to promote goodwill and a cooperative approach to problem solving and conflict resolution. In order to achieve and thus ease the security scenario, ILRI shall design plans for:

- Responding to approaches from the community
- Responding to community action against ILRI

CONTRACTORS

Contractors are required to comply with ILRI's security plans and demonstrate that security risks which fall within their contractual domain have been reduced to an acceptable level, and that they are prepared to commit the necessary manpower and resources to ensure compliance. ILRI CSO will conduct regular security assessments of contractors' facilities and operations on site, reporting any security malpractice to management. Contractors will not be permitted to resume operations until such practices or conditions have been corrected. All contracted staff on site shall display their passes at all times and will not exit the premises while still in their overalls.

INFORMATION AND COMPUTER SECURITY

ILRI's assets include substantial quantities of confidential information which the ICT Manager will identify and ensure that appropriate protective measures are introduced and enforced. It must be reiterated that confidential information of any nature must only be released subject to appropriate authority.

Employees are required to maintain confidentiality with respect to information and knowledge. All employees prior to commencing work for ILRI must sign a confidentiality statement/agreement. A confidentiality clause shall be a standard feature of all employment and consultant's contracts.

CARRYING CASH

Staff may obtain and carry official cash for purpose of paying third party expenses where payment by bank transfer and cheques is not possible. Staff may also carry cash relating to their own per diems to cover costs relating to accommodation, meals, local travel within the place of mission or field work and to cover sundry expenses.

ILRI staff may carry cash up to a maximum limit of USD 3,000 for official purpose. Staff may carry the required per diems amount to cover their own costs. These amounts may be revised accordingly upon consultation between Finance and the relevant Director.

Staff shall liaise with ILRI Finance department to use non-cash facilities where official funds required are in excess of USD 3,000. These non-cash facilities include prepaid cards, credit cards, and others that ILRI has/will negotiate with banks and mobile money companies from time to time.

MAIL HANDLING

All persons who receive mail should be familiar with the characteristics of letter and parcel bombs and bio-hazards. They should also be briefed on the handling of mail suspected of containing an explosive device or suspected bio-hazard and this activity should be housed at an isolated location.

MEDICAL SERVICES

In most areas where ILRI operates, one of the greatest threats to employees will be from injury or illness.

The procedure for a medical emergency will be to:

- Provide life-saving first aid
- Stabilize the injured or ill person
- Assess further treatment options
- Evacuate to further medical attention if necessary and advisable
- ILRI Human Resources (Health and Safety Unit) in conjunction with the Security Unit are to be notified immediately and will co-ordinate emergency medical evacuation

SECURITY PHASES

ILRI relies on five specific security phases to describe the security measures to be implemented based on prevailing security conditions in a given country or in part of it. This rating acts as a very basic indicator of the required level of evacuation preparedness as well as the overall level of safety and security in a given location. The five phases are:

Phase One: Precautionary

This phase is designated to warn staff members that the security situation in the country or a part of it is such that caution should be exercised while undergoing normal business. All unnecessary travel to volatile areas of the country should be rescheduled (or rerouted) whenever possible. ILRI staff are encouraged to use alternative methods of conducting business whenever and wherever practical (i.e. teleconferences or meetings in other venues located in less volatile environments). Individuals wishing to travel to a country under phase one should obtain security information prior to their departure.

Phase Two: Restricted Movement

This phase signifies a much higher level of alert and imposes major restrictions on the movement of all staff members and their families. During phase two, staff members and their families will be required to remain at home unless otherwise instructed. No travel, either incoming or within the country will occur unless specifically authorized by a Director as essential travel. Phase two is generally of short durations, after which the phase will return to less restrictive terms, or will be increased because of threat.

Phase Three: Relocation

Phase three indicates a substantial deterioration in the security situation, which may result in the relocation of staff members or their eligible dependents. When phase three is declared, the Crisis Management Team [CMT] may recommend any of the following actions:

1. Temporary concentration of ILRI staff in primary locations and onward movement to secondary locations.

2. Relocation of all internationally recruited staff (IRS) members and their eligible dependents to alternative locations within the country and/or
3. Evacuation outside the country of all eligible dependents of IRS. ILRI employees planning on travelling to the country under phase three must obtain written authorization from the director general prior to commencing their travel.

Phase Four: Program Suspension

In this phase, operations in the location have been suspended and all remaining IRS are evacuated.

Travel to the location is forbidden unless there is an overriding reason for the trip. The individual requesting the travel authorization must submit a written justification of the trip vis-à-vis the serious potential risks involved, as well as the necessity of conducting the trip versus other options. Written authorization must be obtained from the director general prior to commencing the trip. Failure to
obtain appropriate authorization for travel to high-risk areas is a potential ground for dismissal.

Phase Five: Evacuation

In this phase, operations in the country have been suspended and all remaining IRS will be evacuated.

If the Director General (or designate) deems it appropriate, essential NRS and their dependents may be evacuated to a pre-determined location.

CRISIS MANAGEMENT PLAN (CMP)

ILRI Management shall develop an Institute Crisis Management Plan
http://ilrinet.ilri.cgiar.org/Datafiles/files/Operations/ILRI%20Crisis%20Management%20Plan.pdf, and a location specific CMP for each location where it operates, covering foreseeable emergency scenarios. The aim of the CMP will be to allow management to make a structured and measured response to incidents and crises as they occur.

The CMP outlines:

- The decision-making authority
- The establishment, composition and responsibilities of the Crisis Management Team (CMT) and the Crisis Response Team (CRT)
- The processes for gathering and disseminating information
- The resources available to the CMT and CRT
- Crisis and emergency response procedures
- Contact details

CRISIS RESPONSE PROCEDURES

ILRI shall establish crisis response procedures which will provide the framework for an immediate, pre-determined response to an emergency or crisis by security and management personnel. This enables time-critical actions to take place while, if necessary, the CMT and CRT prepares to manage the incident.

Procedures may include the management of:

- Armed robbery
- Arrest
- Bomb threat
- Community action
- Fire
- Kidnap and abduction
- Medical evacuation
- Missing person
- Missing vehicle
- Road traffic accident
- Vehicle hijack
- Extortion threat
- Disease outbreak
- Civil unrest

Security shall issue emergency contact details and have them accessible to staff and all other individuals associated with ILRI (see annex III).

EVACUATION PLAN

ILRI shall develop a detailed staff Evacuation Plan http://ilrinet.ilri.cgiar.org/Datafiles/files/Operations/ILRI%20Evacuation%20Plan.pdf. This plan will include the organization and functions of the ILRI Warden System which may also be used on an ongoing basis as a tool for other security functions.

ALL staff must provide details of directions to their homes and updated cell phone numbers to the Security Unit and Regional Reps.

Evacuation Plan will include:

- Planning details
- Authorizations
- Organization
- Warden system
- Alert status
- Security levels and phases
- Triggers
- Evacuation options
- Coordinating instructions
- Administrative instructions
- Contact details

KIDNAP, ABDUCTION AND EXTORTION

ILRI will not permit an environment that facilitates extortion or kidnap of its employees or their families, nor will it tolerate corrupt practices. The first line of defense against such incidents is self-protection and awareness of the individual and their dependents. In order to help its employees understand the challenges of life in the field environment, ILRI will ensure that appropriate security training is available.

However it is possible that, through an unforeseen train of events, employees could be subject to kidnap attempts. The outcome of such attempts will depend on the employees' alertness, response and, subsequently, full reporting of the incident to the ILRI Security Unit and the relevant authorities. Should such a kidnap attempt be successful, ILRI's clear and unambiguous policy is to obtain the safe release of the employee in conjunction with the host country's security agencies or, where appropriate, internationally recognized global risk and crisis management companies.

TRAINING

The Security Unit and the HR Unit will develop and share online security and safety courses and modules, performance standards and performance indicators for all staff and will develop and document a training plan which ensures staff will be assessed at regular intervals based on their lines of work.

Awareness

Security awareness is a key factor in ILRI's security plan. All staff are to be informed of the risks that they are exposed to and the security measures that are in place, so that they can take both personal and collective measures to protect themselves.

Specific Role Training

Training specific to the role of certain staff should be given on a regular basis. The Security Unit will test security staff using scenario training exercises. Training programs will be designed for the following staff:

- Crisis Management and Response Teams
- Drivers
- Security Officers
- Guards
- Wardens

All security staff will be trained to administer first aid and Crisis Response Procedures

SECURITY AUDIT

Security arrangements for ILRI are to be the subject of formal audits.

Frequency of Security Audits

Security audits are to be undertaken at both campuses and all regional offices on either of the following occasions:

- Every year
- Following a major change (including expansion or contraction or relocation) in operations or staffing
- Following a serious security incident
- Following the receipt of a security threat

ANNEX I: ILRI KENYA SECURITY INSTRUCTIONS

Security Procedures

Instructions on security matters affecting all personnel, including campus access control, vehicle parking and the safeguarding of information and search procedures are contained within the Standard Operating Procedures (SOP)

The SOP defines individual responsibilities for security, the reporting structure, and the duties and authority entrusted to each security staff member in relation to his appointment and post.

ILRI Campus Security

ILRI Campus Security is a hybrid system comprising of in-house Security Officers and a contracted guard force. A written security instruction is in place for the ILRI Kenya Campus. In particular, this covers the action to be taken in the event of threat or actual emergency. Responsibilities for security and the procedures to be followed at ILRI Kenya Campus will be set out clearly and should include:

- Access/Egress control of staff, visitors, contractors, suppliers and vehicles
- Perimeter patrol, integrity and inspection
- Powers of search and apprehension of suspected persons
- Reporting and recording of incidents
- Contingency plans for responding to security threats or incidents
- Security training and awareness requirements

Physical Security

The physical security of ILRI Campus –Nairobi will be paramount and will include perimeter security fence, access control systems, lighting, surveillance system, appropriate manned guarding, dogs, communications and control room equipment. This will assist the security team in deterrence, detection, delay and response to security breaches as they occur.

Access Control and Identification Cards

The aim of access control is to prevent unauthorized access to the campus and restricted areas while causing the minimum disruption to operations. Certain key points or areas shall be identified and varying levels of access required.

All staff members/personnel/students at ILRI campus and all hosted institutions SHALL, unless specific reasons dictate otherwise, CARRY and DISPLAY, valid ILRI staff identification/access cards. Access authorization shall be amended or cancelled when the employee in question ceases to work with ILRI. This applies to all staff, students, consultants, temps and casuals.

Visitors shall always be registered and authorized to access ILRI premises by a well identified host through personal telephone extension or through e mail. Access to visitors will be authorized only after receiving communication from the host staff member.

Visitors shall be registered and issued with a specific- to- area visitors ID in exchange of formal identification document. Visitor ID’s must be visibly displayed at all times

Visitors shall report back to the main gate after their visit with a signed visitors pass. They will then return the visitors ID and reclaim their identification document.

Dependants of staff may be issued with ILRI dependants ID and shall always display it while on any ILRI premises

Gate Pass

The Gate Pass (GP) system is designed to reduce the unauthorized removal of ILRI Owned Equipment (ILRIOE) from the campus. The system for the removal of ILRIOE no longer requires advanced clearance from ILRI Security, before the equipment can be removed. The system shifts the onus for the removal of ILRIOE from inside of the campus to the Heads of the ILRI Departments, Hosted Institutions or Designated Representatives. They are now the authorizing persons and must sign the gate pass request through e mail and forward to the security helpdesk.

The gate pass is an official ILRI document held only by the Security, Farm and occasionally the Facilities Units. All details of the items to be removed must be included and signed off by the respective authorized officers in these units. Thereafter, a reconciliation of the gate passes issued and the requests will be done by the Security Unit.

a. Access Control to Laboratories and Buildings

ILRI will be divided into the following sectors each with its own access control protocols

- Laboratories
- Data/communications/engineering areas
- Offices
- Administration
- Service

Special attention will be paid to the laboratories. They will be classified as restricted areas and access protocols will vary depending on the bio-security level of the Lab.

Visitors to these areas WILL always be accompanied by an authorized staff member and they will have to adhere to the security and safety procedures in place.

ALL STAFF AND VISITORS WITHIN THE LABS WILL ALWAYS DISPLAY THEIR IDs AT ALL TIMES. THIS INSTRUCTION WILL BE STRICTLY UPHELD.

UNAUTHORIZED ACCESS TO THESE AREAS IS STRICTLY PROHIBITED
Access to the other areas will be monitored and recorded from the security control room and adherence to protocols and instructions is required from all users.

Refer to the Access Control SOP

Key Control and Management

All keys to all doors within the campus shall be under the initial custody of the Security Unit. The Security Unit will keep all keys under lock and key and only the Duty Security Officer will have access and allowed to open and secure doors.

Copies of keys requested by staff to offices shall only be issued after a proper determination has been made as to whether the keys are required.

If a staff member is vacating an office and is in possession of a key, he/she will surrender the key to the supervisor/Administrative Assistant and will sign. If the key is not going to be reassigned to another user, the supervisor/administrative Assistatant shall submit the key to the Security Unit for safe custody.

No member of staff is allowed to make copies of keys to any door within the campus without authorization. All copies will be made by the Security Unit after a request has been made the relevant supervisor and has been duly approved by the CSO after a needs assessment has been made.

Depending on the need or after a risk assessment, some locks to certain doors will be changed and new keys issued to the new, continued or relevant users.

Hosted Institutions

All institutions hosted on ILRI Nairobi Campus will adhere to the ILRI security regulations, standard operating procedures and instructions, access control procedures and general directions of the security unit as they may be given from time to time.

Acceptance of Legal documents on behalf of ILRI and ILRI Staff

The Host Country Agreement (see extract of Article IV(1 to 5) of the HCA below) grants the Director General sole control of ILRI facilities including the right to allow or deny entry to ILRI premises. Under Para 2, even government officials may not enter ILRI premises to carry out any official duties without observing the conditions that ILRI (through the DG) has laid down to allow or deny entry to such officials.

Para 5 however covers situations where a messenger delivers to ILRI by hand a Court Summons or any other official correspondence addressed to ILRI or a staff member who is within the premises. So as not to contravene Para 5, ILRI Security will accept delivery (but not allow entry) of hand delivered official communication/letters. Otherwise refusing service of such official communication may be deemed to run foul of Para 5, as abetting avoidance of service of legal process, whether to ILRI or members of staff.

Therefore in instances where letters and in particular communication such as court orders (from any court) or correspondence from a lawyer (in a suit against ILRI) is delivered to the gate on foot, such letters should be received (and stamped with an ILRI receive stamp indicating date and time and name of receiving security officer and signature) and recorded. Particularly for court summons, this will be brought immediately to the attention of the DCS, DHR and the Legal Officer who will then take the matter up from there.

In the event that the summons is to an individual (Staff Member) and not to ILRI, the same procedure will be followed. The following section from the Host Country Agreement shall prevail. It reads as follows:

ARTICLE IV
Inviolability of the Facilities.

1. *The land, offices, laboratories, buildings and other property of ILRI or forming part of its facilities shall be inviolable and shall be under the sole control and authority of the Director General.*

2. *No official of the Government, whether administrative, judicial, military or police shall enter ILRI to carry out any official duties except with the consent of, and under conditions agreed to, by ILRI through the Director General.*
3. *All records, correspondence, documents and other materials of ILRI shall be inviolable.*
4. *ILRI shall have the power to make regulations applicable within its facilities in order to establish therein all necessary conditions for its operation.*
5. *Without prejudice to the provisions of the present Agreement, ILRI shall prevent its facilities from becoming a refuge for persons avoiding arrest under the laws of Kenya or who are required by the Government for extradition to another country or for persons who are endeavoring to avoid service of legal process.*

Outline management and control of investigations

In the event of security breaches and incidents, ILRI's own internal security system will conduct investigations. ILRI CSO has the overall control of investigations, but may delegate the responsibility for the day-to-day follow ups to the Duty Security Officer (DSO). The CSO is responsible for the management, control and supervision of all tasks relating to investigation. In some cases of a criminal nature, the CSO may deem it necessary to involve the jurisdictional police or the Diplomatic Police unit, but before this, each case should be assessed in consultation with the DCS. The CSO should also advise on legal implications. Below are some basic guidelines for internal investigations:

The ILRI CSO is responsible for the smooth running of investigations. ILRI CSO is responsible for ensuring that Security Unit resources are properly utilized and maintained during investigations.

The Security Officers are responsible for submitting to the CSO timely and accurate investigation reports. They are also accountable for the use and maintenance of other Security Unit resources.

Cases investigated by ILRI Security Unit will include:

- Unnatural death or injury to ILRI staff, dependants and those covered by the ILRI security umbrella
- Unnatural death or injury to third parties when ILRI staff, dependants and those covered by the ILRI security umbrella are involved

- The occurrence or discovery of any loss or damage to ILRI equipment, stores or other property (except items on personal issue), which cannot be attributed to fair wear and tear
- Loss of or damage to property of a third party when ILRI personnel are involved
- Unnatural death of ILRI staff or death of a third party that involves ILRI staff (not including fatal traffic accidents)
- Alleged sexual offences (not sexual harassment) where ILRI staff are either accused or are the victims. (Sexual harassment cases are to be dealt with by HR in the first instance)
- Serious assaults and assaults involving weapons in which ILRI staff are involved.
- Possession, procurement, distribution or use of narcotics or other illegal substances involving ILRI staff
- Smuggling and or the sale of contraband goods by or to ILRI staff currency offences
- Serious injury to, or caused to a third party by, ILRI staff
- Possession of unauthorized weapons involving ILRI staff
- Any incident or altercation involving citizens of the host nation and ILRI staff burglaries and thefts of ILRI property and equipment
- Any incident directed by ILRI management that requires detailed investigation

Investigation procedures

Immediately after any of the above incidents are reported to security, the CSO will brief the DCS as soon as possible and submit an initial preliminary incident report. Based on that brief, the DCS will then advise on whether immediate internal investigations should be launched. In the event that investigations are to be launched, the CSO will — through the supervisor of the affected staff member — summon, interview and acquire written statements from all suspects and witnesses involved in the case. Sometimes, there may be a need to have the suspect(s) and witness(s) re-interviewed and further statements recorded, but if so, this should be explained to the supervisor of the affected staff so that they can be released from duty for this second session. All staff and campus users are required to cooperate with investigations when requested to do so.

Immediately after the investigations are completed, a full investigation report, with attachments if any, will be submitted to the DCS and DHR and copied to the supervisor of the staff member affected. Such a report will be confidential and will be handled on an exclusively 'need-to-know–need-to-use basis. Based on the available evidence or lack of, the report can be used for internal administrative procedures.

The main objectives of a security unit led investigation are:

- Document the incident
- Recover evidence
- Maintain integrity during the process
- Protect the rights and liberties of all involved
- Determine the facts
- Advise on appropriate actions

ILRI Vehicle and Bus Use

All vehicles will be correctly maintained according to the manufacturer's schedule of maintenance. All occupants will wear seat belts. Vehicles will only be hired through providers authorized by ILRI management. Vehicles will be secured when not in use. Procedures will be implemented to guard against theft, damage and abuse. International staff must first be certified to conform to driving laws of the host country before being allowed to drive in foreign countries. Duties involving night driving shall strictly enforce such restrictions. Where non-locals are authorized to drive they will ensure that all necessary permits and licenses have been obtained. Violations of this policy will subject employees to disciplinary measures.

Staff buses are beneficial to:

- ILRI permanent staff
- Temporary staff
- Hosted Institutions staff
- Temporary staff
- Domestic staff of campus residents
- Residents

Outsourced staff and contractors are <u>NOT</u> authorized to use the staff buses.

The above named users will be required to identify themselves to the security officers manning the doors before they board the buses both to and from ILRI.

Staff who engage in behavior likely to place both the driver and his/her fellow staff members in danger shall be asked to disembark from the vehicle by the driver in consultation with the Chief Security Officer. The staff member shall also face disciplinary measures.

Use of abusive language to the driver, other users or to the security officers is also prohibited and will also attract disciplinary action.

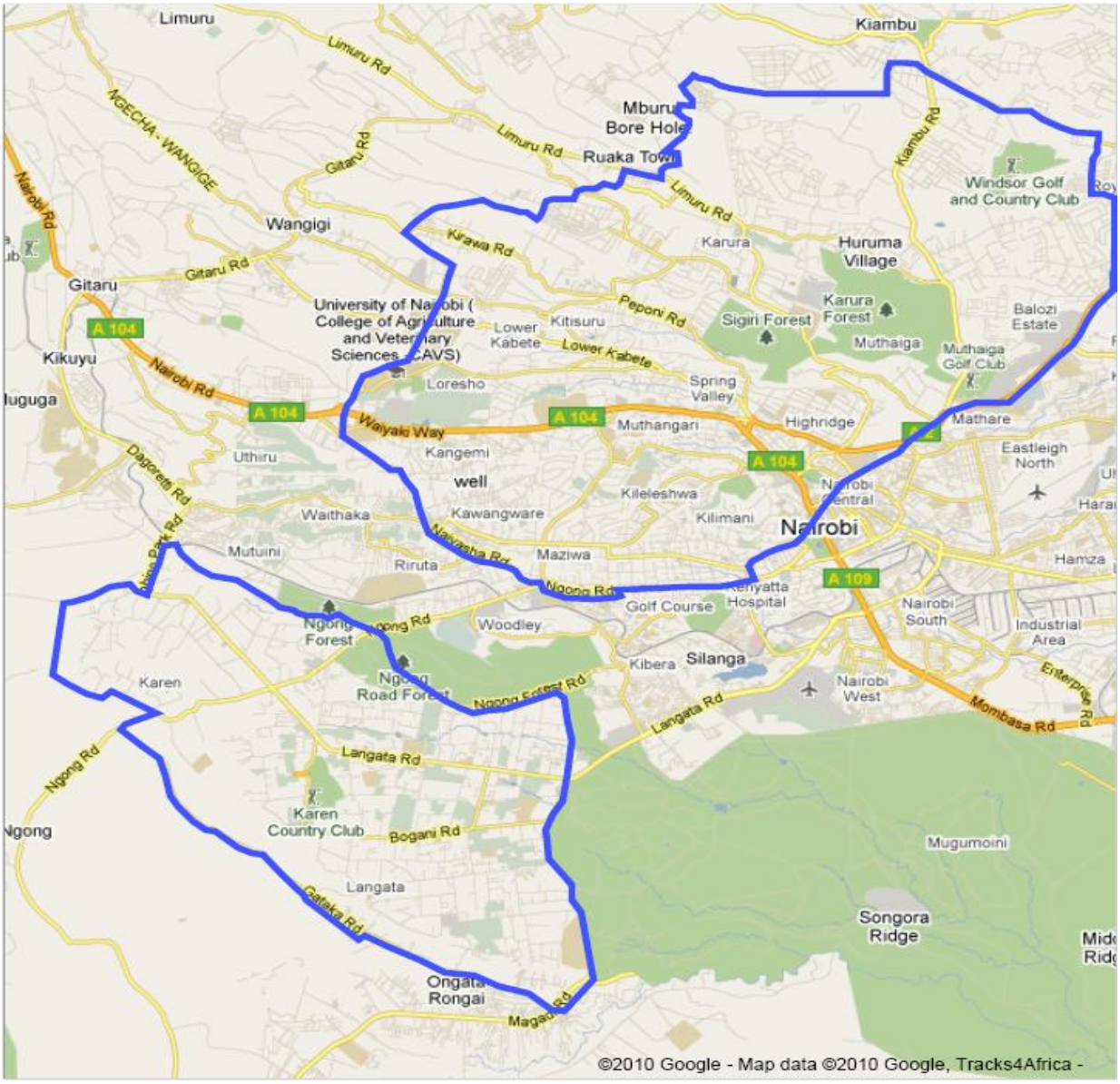
Residential Security

In order to comply with ILRI security standards, internationally recruited staff (IRS) are advised to live within designated residential areas for international staff. Off campus, these should be areas that have relatively secure environments and the fact that police and other emergency services have good response times to those areas. These areas are essentially known as the **'Blue Zones'**. Nationally Recruited Staff (NRS) have the liberty to choose preferable residential locations in any part of the country.

The integrity of the dwelling structures should also adhere to minimum acceptable physical security standards.

Contracting of guarding and alarm services at staff residences off campus will be advised by the Security Unit. Preferably, guarding services at the residences will be performed the the same company contracted on campus and alarm services will be performed by a different company.

ILRI Security Unit will arrange for residential security surveys to be carried out prior to occupation or at any time on request.


Limuru
Limuru Rd
Kiambu
AGECHA - WANGIGE
Mburu
Bore Hole
Ruaka Town
Limuru Rd
Kiambu Rd
Gitaru Rd
Windsor Golf
and Country Club
Nairobi Rd
Wangigi
Karura
Huruma
Village
Kirawa Rd
Gitaru
Gitaru Rd
University of Nairobi (
College of Agriculture
and Veterinary
Sciences (CAVS)
Lower
Kabete
Kitisuru
Peponi Rd
Sigiri Forest
Karura
Forest
Balozi
Estate
A 104
Kikuyu
Nairobi Rd
Lower Kabete
Muthaiga
Muthaiga
Golf Club
Loresho
Spring
Valley
A 104
A 104
Waiyaki Way
Muthangari
Highridge
Mathare
Daggretti Rd
Uthiru
Kangemi
Eastleigh
North
well
A 104
Kileleshwa
Kilimani
Nairobi
Waithaka
Kawangware
Mutuini
Riruta
Maziwa
Ngong Rd
A 109
Hamza
Golf Course
Hospital
Nairobi
South
Industrial
Area
Ngong
Forest
Woodley
Kibera
Silanga
Karen
Ngong
Road Forest
Ngong Forest Rd
Nairobi
West
Langata Rd
Mombasa Rd
Ngong Rd
Langata Rd
Karen
Country Club
Bogani Rd
Mugumoini
Langata
Songora
Ridge
Ongata
Rongai
©2010 Google - Map data ©2010 Google, Tracks4Africa -

ANNEX II: ILRI ETHIOPIA SECURITY INSTRUCTIONS

Security Groups

To help in effectively safe guarding ILRI and Hosted institutions staff and properties, the Security Unit is organized in four different Security Groups to perform its duties on 24 hours basis.

Theft or Break-In

During this incident, security officer/group leader with the knowledge of Head of Operations calls the police professionals to investigate. Since the custodian of the missing items/goods/assets is responsible for the assets under their control, they are the first people to be contacted.

ID Cards Control at the Main Gate and On the Campus

All ILRI/Hosted institutions staff are required to display their respective ID cards on the campus.

Casual workers, daily labourers and contracted staff are also required to clearly and visibly display their respective ID cards

The external info centre users, visitors/guests surrender their respective National ID cards at the main gate and are issued with ILRI-info centre / ILRI visitor pass cards respectively to be visibly displayed.

Participants of seminars, workshops and meetings will be checked on arrival at the main gate against their respective name lists provided in advance to the security office.

Non ILRI/Hosted institutions staff residing on the ILRI campus should produce their "Resident Guests" ID card ate the main gate whenever they come in to the ILRI campus. (This ID card will be provided by housing and catering manager).

Non ILRI/Hosted intuitions staff coming in, going out on foot carrying bags or plastic bags, the bags should be checked and searched thoroughly by the security staff on duty at the main gate.

ID cards or Entry passes for the household staff (drivers, maids, gardeners) will be issued by Human Resources Unit by the request of the employee's and copies of the ID cards will be sent to the security office for file and follow up at the main gate.

All Zebu Club members are required to produce their membership cards at the main gate whenever they come in. Their names will be checked by the duty Security Group Leader/security guard at the main gate against the list of names provided by the Zebu Supervisor.

Guests/visitors will not be allowed into offices between 0645 and 0815 hrs.

Zebu Club members will not be allowed onto campus between 2200 and 0700hrs.

Registry of attendance for week-ends and public holidays is provided at the main entrance of the Administration building for those staff who work on the weekends and public holidays.

Gate Pass Control

To control the movement of any ILRI/Hosted institutions items/goods/assets leaving the campus, the following procedures are implemented:

- Any property taken out of the campus must have gate pass duly signed by the authorized supervisor.

- This duly signed gate pass by the authorized supervisor will be given to the duty Security group Leader/Security Guard at the main gate or to the duty security staff at the bus stop for employees using the service buses.
- During the checking of the loaded items, goods/assets by the security, any discrepancy between the duly signed gate pass and loaded item/s it will be immediately reported to the security officer. The security officer reports to Head of Operation for appropriate decision the items may be confiscated until further investigation/clarification or call local police for further investigation.
- The authorized signatories' specimen signatures will be sent to the security office by the Units/Departments Heads.
- Personal items coming or going out of the ILRI campus will be registered at the main gate on the log book provided for this purpose.
- No ILRI vehicle will leave the campus without duly signed vehicle movement order.

Internal Investigations

The task of the internal investigation team:

- Internally investigate the Security problems, theft, and misconduct.
- Collect information and circumstantial evidences.
- Talk to office holders, the concerned duty staff at the incident area.
- Give additional information to the police investigation team.
- Give a report on the incident.
- Give administrative recommendations.

ANNEX III: KENYA EMERGENCY CONTACTS

ILRI Security Helpdesk	+254-(20) 422 3362 +254 711 033362	EMERGENCY HOTLINES +254 728 970 722 +254 733 634907
ILRI EHS Office	+254-(20) 422 3375 +254-(20) 422 3883 +254-(20) 422 3887	
Skype	ILRI Kenya Security	
Aga Khan Hospital MP Shah Hospital Avenue Hospital Nairobi Hospital	Tel: 3740000 Tel: 3742763/7 Tel: 3742907/3745750 Tel: 2845000/284/6000	
Kenya Red Cross Emergency Plus Medical Services	+254-3950395 +254-0700 395 395	Mobile: +254-0725-380136
Kenya police control room	+254-2724154	
Diplomatic Police Unit	+254-2724133	Mobile: +254-0716-000559 / +254-0731-170666
Kenya Army-Kabete	+254-4444477	
St Johns Ambulance	+2564-2210000/2244444	Mobile: +254-0721-225285
G4S Control Room	+254-6982999	Mobile: +254-0733-900030/ +254-0723-786565

ANNEX IV: ETHIOPIA EMERGENCY CONTACTS

NAME	TELEPHONE NUMBERS	
	DIRECT	*Free call*
Addis Ababa Fire Brigade	0116-63-19-98	939
Addis Ababa Fire Brigade	0116 63 03 73	
Bole Sub-city Fire Brigade	0116-63 03 73/ 74	
Addis Ababa Police Commission	0116-61 05 05 0116-63 00 63 0116-61 01 11	991
Traffic Police Investigation Unit	0116-62 82 22 0116-62 8086	945
Bole Sub-city Police Dept.	0115-53 67 58 0115-50 95 48	
ILRI Chief Security Officer	0911-41 25 56	