Crisis Management Policies and Procedures

1 April 2023

Contents:

Background

The Crisis Management Policies and Procedures Manual is a basic guide to providing a response system, by the Crop Trust, to a major crisis or emergency occurring to the Crop Trust or to Crop Trust Staff. All personnel designated to carry out specific responsibilities are expected to know and understand the policies and procedures outlined in this plan. The response to any major crisis or disturbance will always be conducted within the framework of this plan.

This Manual refers to notifications of persons responsible for the Organization in the absence of senior management. Please ensure that you also consult the Administrative Circular currently in force that indicates the up-to-date list of persons who are responsible in such cases.

Purpose

The Crisis Management Plan is designed to effectively coordinate responses in order to protect life and property during and immediately following a major crisis, emergency or disturbance. It is placed into operation whenever an emergency occurs affecting the Organization or its Staff.

These procedures are designed to prioritize human safety and to exercise maximum due diligence in securing Crop Trust assets. While the procedures cannot take into account all eventualities, they are intended to provide a framework for sound decision-making in evolving circumstances.

Crisis Types

For the purposes of this plan there are 3 types of crises:

1. **Threat to Staff security**
   - 1.1 Serious injury or death of a Staff Member (whether during or outside of work hours) or case of a missing Staff Member
   - 1.2 Threats to Staff safety due to behavior of others (Irrational/dangerous behavior of a Staff Member that threatens other Staff, Intruders exhibiting dangerous behavior, terrorist threats)

   There are other important threats to Staff safety such as fire, flood, earthquake, other natural disasters, accident/first aid issues and travel safety (vaccinations, etc.). Such situations are covered in the Occupational Health and Safety manual.

2 **Compromised data/IT security breach** - this comprises situations that relate to:
   - 2.1 Financial data breach
   - 2.2 Security breach involving other (non-financial) data

3 **Threat to Crop Trust resources or property/assets**
   - 3.1 Loss or theft of office keys
   - 3.2 Loss or theft of Crop Trust property (laptop or other equipment)

Below are guidelines on procedures to be followed for these threats.

Use of this manual

Due to the nature of crises, in many cases, Staff will not have time to read this manual at the time of a crisis event. Therefore, the Crop Trust requires that Staff read this manual fully and familiarize themselves sufficiently with the policies procedures contained herein.

A copy of this manual should be kept by each Staff Member in a place that is easily accessible. All Staff should post the separate list of Crop Trust emergency focal points (available from the Corporate Operations team) near their desk in plain view.

1. THREATS TO STAFF SECURITY

Areas under this threat fall primarily under the following categories (covered in this manual):

1.1 Serious injury or death of Staff Member, or case of missing Staff Member
1.2 Threats to Staff safety due to behavior of others

As mentioned, threats to Staff security resulting from first aid emergencies, fire or other disasters are covered in the Occupational Health and Safety Manual.

1.1 Serious injury or death of Staff Member, or case of missing Staff Member

Notifications:
In cases of serious injury or death of a Staff Member or in cases where a Staff Member has not reported to work (see conditions below) or is suspected missing, Chief of HR and Corporate Operations should be immediately notified either in person or by telephone who will take appropriate action as indicated below and notify the Director of Administration and Executive Director. In the absence of the Executive Director, the person responsible for the Organization must be notified (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Required actions and responsibilities:

Staff Members:

- In cases where a Staff Member becomes aware that a colleague has been seriously injured or died they must immediately notify the Chief of HR and Corporate Operations either in person or by telephone (who will notify both the Director of Administration and the Executive Director, or in case of travel the person in charge of the Institute).
- In cases where a Staff Member becomes aware that a colleague has not reported to work within the usual timeframe they must contact the Corporate Services office to ascertain whether the person has notified of the delay, has been authorized to work from a remote location or has authorized leave on file. Where this is not the case and the delay exceeds four hours, the Staff Member must notify the Supervisor (or their delegate) either in person or by telephone of the Staff Member who has not reported to work as usual.

Supervisors:

- The Supervisor must immediately attempt contact the missing Staff Member by telephone in order to obtain information regarding their safety. In case the Staff Member cannot be reached, the Supervisor must notify the Chief of HR and Corporate Operations immediately either in person or by telephone.

Chief of HR and Corporate Operations

- If the Staff Member cannot be reached by telephone by their Supervisor, the Chief of HR and Corporate Operations must attempt to locate the person by contacting cohabiting family members if appropriate and/or arranging for staff to go to the person's residence and if necessary.
- In case the Chief of HR and Corporate Operations has not been able to contact the Staff Member or cohabiting family members they will notify both the Director of Administration and Executive Director (or in case of travel, the person in charge of the Institute) and, in consultation, assess actions to be taken including, as appropriate, alerting police and family members nominated by the Staff Member as emergency contacts. In all cases, the

Executive Director should be notified as soon as possible thereafter by the Chief of HR and Corporate Operations.

In case of accident or death, the actions by the Chief of HR and Corporate Operations will include:

- Organizing hospital or home assistance if needed.
- Contacting the person identified by the Staff Member (on the Personal Information form) as their emergency contact (in cases of very serious illness or death). Where the Staff Member is unconscious or unable to give consent to contact the emergency contact, the Corporate Operations team will automatically contact this person.
- Contacting the medical insurance company if hospitalization is required in order to assist with obtaining pre-authorization or handling other arrangements, or assisting the Staff Member's family with this issue.
- In case of death, organizing necessary arrangements for transportation of the body from the place of death to the deceased's home city and country (as per Section 7 of the Personnel Policies and Procedures Manual).

1.2 Threats to Staff safety due to behavior of others

Please note that this section of this Manual addresses only those crisis situations where a Staff Member's physical well-being is at immediate risk. Policies and disciplinary measures with regarding to harassment, intimidation and discrimination are covered in the Personnel Policies and Procedures Manual Section 2.3 (Conduct of Staff Members) and Section 11 (Disciplinary code).

This section of this Manual serves to provide guidelines on procedures for crisis situations involving Staff safety. It cannot cover all possible scenarios of crisis situations and Staff are expected to use their best judgment in assessing situations in which either they themselves or other Staff are at risk. In considering what kinds of interventions are necessary for a particular situation, Staff are expected to first consider their own safety and then the safety of others. A Staff Member must not intervene in a situation where it is clear that they will put themself at risk of injury or death.

It is critical for Staff to understand the importance of informing police as soon as it is possible and safe to do so and once matters have come to a situation of stability and safety that they immediately inform the Executive Director and Chief of HR and Corporate Operations (who will inform the Director of Administration).

1.2.1 Irrational/dangerous behavior of a Staff Member that threatens other Staff

Examples of such threats may include (but are not limited to):

- Suicide threat or attempt;
- Assault or threat of assault;
- Irrational behavior that appears dangerous.

Notifications:
In such cases, the Executive Director and Chief of HR and Corporate Operations should be notified immediately either in person or by telephone (who will also notify the Director of Administration). In the absence of the Executive Director, the person responsible for the Institute must be notified (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Required actions:
Any person in authority nearest the site of the incident must take the following action (note - persons not "in authority" should also take action if common sense so dictates):

- Assess the situation and level of danger to the Staff Member or to others;
- If the situation poses risk to one or few Staff Members and it is felt that the situation will not affect others in the office or that it will be unnecessary or dangerous to conduct a general Staff evacuation, then:
    - Emergency services should be called as soon as it is safe and possible to do so
      POLICE – Tel: 0-110 – be prepared to answer detailed questions to describe the location and description of the event.
      Our address: Platz der Vereinten Nationen 7
    - Assess (based on the situation and as common sense dictates) whether it is possible or useful to intervene. If it is assessed that direct intervention would be safe, useful or required then (depending on the situation):
        - Ask other colleagues for assistance as/if necessary;
        - Stay calm, do not threaten, frighten or antagonize the person(s) involved but try to talk/reason and calm down the person displaying irrational or threatening behavior to bring the situation to one of non-threat to human safety;
        - Important – Staff Members should not risk to intervene if doing so would put the Staff Member or others at risk.
- If the situation poses risk of immediate threat to the safety of others more generally, then an evacuation may be deemed the most appropriate course of action. In such cases, an evacuation order should be initiated (all Staff have authority to initiate a required evacuation):
    - an evacuation order should be given by notifying any Staff Member who is trained in occupational health and safety emergencies, who will be able to assist in conducting the evacuation according to emergency protocols used for fires and other emergencies). A list of Staff trained in emergency procedures is provided on the Emergency Contact Sheet posted in all common areas and all Staff should have a copy of this posted near their desk (available also from the Corporate Operations Team). If these Staff are not available or if the situation requires immediate evacuation, then the Staff Member observing the behavior should proceed to alert Staff to evacuate as quickly as possible by taking calm and decisive steps to contact all Staff in the building (if it is possible, the Staff Member should enlist other Staff to alert nearby colleagues to assist with this).
    - Emergency services should be called as soon as it is safe and possible to do so
      POLICE – Tel: 0-110 – be prepared to answer detailed questions to describe the location and description of the event.
      Our address: Platz der Vereinten Nationen 7
- In case of an evacuation, depending on the nature of the emergency, there are different meeting points for Staff as follows:
    - If it is safe to do so, Staff should assemble at the normally-designated gathering point (on the meadow in front of the building – marked with the emergency assembly sign below):

      

      However, this area is in clear view of the office windows and, depending on the situation, may not be a safe gathering spot.
    - If the situation requires that Staff are kept from view of the offices, then Staff should assemble in front of the World Conference Centre.
    - If neither situation above is appropriate (offer adequately safe distance from the danger), then Staff must use common sense to distance themselves from the source of danger.

- As soon as possible, the Chief of HR and Corporate Operations should ensure that evacuees are present and accounted for. To assist in this, Staff should make there whereabouts known as soon as possible by contacting the Chief of HR and Corporate Operations by phone, text or in person as soon as the situation becomes safe. If they cannot contact the Chief of HR and Corporate Operations, they should contact any other Staff Member and request that the Chief of HR and Corporate Operations be notified as soon as possible.
- The Chief of HR and Corporate Operations should attempt to take a Staff count and request all Staff Members present to alert them to any other Staff who are missing. The police or other emergency personnel should be notified of any Staff who are unaccounted for.
- Under no circumstances should Staff return to the site of danger to search for missing Staff as long as the danger is present. Emergency services personnel must be notified to this and requested to intervene as possible.
- Once the immediate situation has been resolved, the Chief of HR and Corporate Operations must follow up on any residual crisis situation through assessment of required follow-up actions in consultation with the Director of Administration and Executive Director.

Summary of Responsibilities:

Any person in authority nearest the site of the incident:

- Assess situation and take action as outlined above including, as necessary, calling emergency personnel, assist in diffusing the situation (only if safe), initiate or conduct Staff evacuation (if necessary).

Staff trained in emergency evacuation procedures:

- Assist in conducting an emergency evacuation if needed

All Staff:

- Follow safety procedures

Chief of HR and Corporate Operations:

- Assess situation and provide assistance/guidance as needed;
- Take Staff count to ensure all Staff are accounted for;
- Ensure emergency personnel have been alerted;
- Inform Director of Administration and Executive Director (or person in charge of the Institute);
- Once the immediate situation has been resolved, follow up on any residual crisis situation through assessment of required follow-up actions in consultation with the Director of Administration and Executive Director.

1.2.2 Intruders exhibiting dangerous behavior

Notifications:
In such cases, Executive Director and Chief of HR and Corporate Operations (who will notify the Director of Administration) should be notified in person or by telephone as soon as it is possible. In the absence of the Executive Director, the person responsible for the Institute must be notified (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Required actions:
Any person who witnesses or comes into contact with an intruder who is exhibiting dangerous behavior or is perceived to be a threat should:

- Assess whether it is necessary, safe and possible to immediately distance oneself from the intruder (as common sense dictates);
- Assess whether it necessary, safe and possible to ask other colleagues for assistance;
- Stay as calm as possible;
- Important – Staff Members should never risk intervention if such intervention would put the Staff Member or others at risk;
- If the situation poses risk of immediate threat to general human safety and it is possible for the Staff Member to evacuate others (all Staff have authority to initiate a required evacuation):
    - an evacuation order should be given by notifying any Staff Member who is trained in occupational health and safety emergencies, who will be able to assist in conducting the evacuation according to emergency protocols used for fires and other emergencies). A list of Staff trained in emergency procedures is provided on the Emergency Contact Sheet and posted in all common areas and all Staff should have a copy of this posted near their desk (available also from the Corporate Operations Team). If these Staff are not available or if the situation requires immediate evacuation, then the Staff Member observing the behavior should proceed to alert Staff to evacuate as quickly as possible by taking calm and decisive steps to contact all Staff in the building (if it is possible, the Staff Member should enlist other Staff to alert nearby colleagues to assist with this).
    - If it is safe to do so, Staff should assemble at the normally-designated gathering point (on the meadow in front of the building – marked with the emergency assembly sign below):

      

      However, this area is in clear view of the office windows and, depending on the situation, may not be a safe gathering spot.
    - If the situation requires that Staff are kept from view of the offices, then Staff should assemble in front of the World Conference Centre.
    - If neither situation above is appropriate (offer adequately safe distance from the danger), then Staff must use common sense to distance themselves from the source of danger.
- Emergency services should be called as soon as it is safe and possible to do so (by any Staff Member who is able to do this):

  POLICE – Tel: 0-110 – be prepared to answer detailed questions to describe the location and description of the event.

  Our address: Platz der Vereinten Nationen 7
- The Chief of HR and Corporate Operations should be notified in person or by telephone as soon as it is safe and possible to do so (by any Staff Member who is able to do this)
- In cases where Staff have been evacuated, the Chief of HR and Corporate Operations should ensure that evacuees are present and accounted for as soon as possible. To assist in this, Staff should make their whereabouts known as soon as possible by contacting the Chief of HR and Corporate Operations by phone, text or in person as soon as the situation becomes safe. If they cannot contact the Chief of HR and Corporate Operations, they should contact any other Staff Member and request that the Chief of HR and Corporate Operations be notified as soon as possible.
- The police or other emergency personnel should be notified of any Staff who are unaccounted for.
- Under no circumstances should Staff return to the site of danger to search for missing Staff as long as the danger is present. Emergency services personnel must be notified to this and requested to intervene as possible.

- Once the immediate situation has been resolved, the Chief of HR and Corporate Operations must follow up on any residual crisis situation through assessment of required follow-up actions in consultation with the Director of Administration and Executive Director.

Summary of Responsibilities:

Any person who witnesses or comes into contact with an intruder:
- Assess situation and take action as outlined above

Staff trained in emergency evacuation procedures:
- Assist in conducting an emergency evacuation if needed

All Staff:
- Follow safety procedures

Chief of HR and Corporate Operations:
- Assess situation and provide assistance/guidance as needed;
- Take Staff count to ensure all Staff are accounted for;
- Ensure emergency personnel have been alerted;
- Inform Executive Director (or person in charge of the Institute);
- Once the immediate situation has been resolved, follow up on any residual crisis situation through assessment of required follow-up actions in consultation with the Executive Director;
- Once the immediate situation has been resolved, follow up on any residual crisis situation through assessment of required follow-up actions in consultation with the Director of Administration and Executive Director.

1.2.3 Terrorist threats/violent demonstrations that threaten Staff security

Examples of such threats may include (but are not limited to):
- Bomb threats;
- Civil unrest;
- Attack on building and/or assault of Staff relating to demonstrations or terrorist activity.

Notifications:
In such cases, the Executive Director and Chief of HR and Corporate Operations (who will notify the Director of Administration) should be notified as soon as it is possible either in person or by telephone. In the absence of the Executive Director, the person responsible for the Institute must be notified (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Required actions:
Any person in authority must take the following action (note - persons not “in authority” should also take action if circumstances and common sense so dictates):
- Assess the situation and level of danger to the Staff Members or to others;
- Depending on the nature of the threat and level of risk to human safety, assess whether the situation requires:
    A. an evacuation (for example a bomb threat inside the building); or
    B. a lockdown (for example a demonstration or attack occurring outside of the offices).

  More about these specific procedures is provided below.
- In either case, Emergency services should be called as soon as it is safe and possible to do so:

POLICE – Tel: 0-110 – be prepared to answer detailed questions to describe the location and description of the event.
Our address: Platz der Vereinten Nationen 7

A. Evacuation - If the situation requires an evacuation:
   - an evacuation order should be given by notifying any Staff Member who is trained in occupational health and safety emergencies, who will be able to assist in conducting the evacuation according to emergency protocols used for fires and other emergencies). A list of Staff trained in emergency procedures is provided on the Emergency Contact Sheet and posted in all common areas and all Staff should have a copy of this posted near their desk (available also from the Corporate Operations Team). If these Staff are not available or if the situation requires immediate evacuation, then the Staff Member observing the behavior should proceed to alert Staff to evacuate as quickly as possible by taking calm and decisive steps to contact all Staff in the building (if it is possible, the Staff Member should enlist other Staff to alert nearby colleagues to assist with this).
   - In case of an evacuation, depending on the nature of the emergency, there are different meeting points for Staff as follows:
   - If it is safe to do so, Staff should assemble at the normally-designated gathering point (on the meadow in front of the building – marked with the emergency assembly sign below):

However, this area is in clear view of the office windows and is also fairly close to the building. Therefore, depending on the situation, it may not be a safe gathering spot.
   - If the situation requires that Staff are kept from view of the offices, or the situation requires that Staff be distanced further from the building, then Staff should assemble in front of the World Conference Centre.
   - If neither situation above is appropriate (offer adequately safe distance from the danger), then Staff must use common sense to distance themselves from the source of danger.
   - As soon as possible, the Chief of HR and Corporate Operations should ensure that evacuees are present and accounted for. To assist in this, Staff should make there whereabouts known as soon as possible by contacting the Chief of HR and Corporate Operation by phone, text or in person as soon as the situation becomes safe. If they cannot contact the Chief of HR and Corporate Operations, they should contact any other Staff Member and request that the Chief of HR and Corporate Operations be notified as soon as possible.
   - The Chief of HR and Corporate Operations should attempt to take a Staff count and request all Staff Members present to alert them to any other Staff who are missing. The police or other emergency personnel should be notified of any Staff who are unaccounted for.
   - Under no circumstances should Staff return to the site of danger to search for missing Staff as long as the danger is present. Emergency services personnel must be notified to this and requested to intervene as possible.

B. Lockdown
   An emergency lockdown is necessary in situations where there is reason to believe that exiting the offices (a sheltered area) will expose individuals to greater danger

than remaining in place. In case the emergency situation requires a lockdown (the source of the threat is outside the building) then all Staff should:

- Remain calm
- Do not evacuate the building unless you smell smoke or detect other internal threat
- Immediately seek cover in a place away from windows and doors
- Do not gather in open areas or hallways. These ARE NOT areas of shelter.
- Shut the blinds or pull the shades down. Turn off the lights and try to give the impression that the room is empty
- Be aware of alternate building exits if it becomes necessary to flee
- Put cell phones on silent and vibrate in order to be able to receive alerts but not to alert outsiders/external threats to your position in the building
- Do not leave until police or security personnel contact you to confirm it is safe; follow instructions from police or security.

Summary of Responsibilities:

Any person in authority nearest the site of the incident:

- Assess situation and take action as outlined above

Staff trained in emergency evacuation procedures:

- Assist in conducting an emergency evacuation or lockdown if needed

All Staff:

- Follow safety procedures

Chief of HR and Corporate Operations:

- Assess situation and provide assistance/guidance as needed;
- Take Staff count to ensure all Staff are accounted for;
- Ensure emergency personnel have been alerted;
- Inform Executive Director (or person in charge of the Institute);
- Once the immediate situation has been resolved, follow up on any residual crisis situation through assessment of required follow-up actions in consultation with the Director of Administration and Executive Director.

2. COMPROMISED DATA/IT SECURITY BREACH

Areas under this threat fall primarily under the following categories:

2.1 Threats to financial data
2.2 Threats to other (non-financial) data

All Staff have a responsibility to ensure that Organizational data is protected from potential misuse and to comply with all directives regarding handling of data/information and with all document and ICT security measures. A security breach to the Organization's financial data or to the IT System poses a particularly critical risk to the Organization and must be handled swiftly. Failure to comply with the security measures outlined in the ICT manual or with the crisis management measures in this directive may result in disciplinary action.

Below are the procedures to be followed in case of a suspected or confirmed threat to financial and other data.

2.1 Financial data breach

The risk of a security breach involving financial or banking data carries particularly critical risks to the Organization. Any suspected or confirmed breach of financial or banking data must be handled immediately and without delay.

Mitigating risks in connection with breaches of financial data
Where financial or banking data has been compromised or is at risk of threat the procedures to be followed are provided below. Failure to comply with the crisis management measures in this directive may result in disciplinary action.

Notifications:
Any Staff Member who is aware of a real or potential data breach or IT security breach that involves financial or banking data must immediately notify (either in person or by telephone) the Executive Director and the Chief of HR and Corporate Operations (who will notify the Director of Administration). The Chief of HR and Corporate Operations will constitute a Crisis Management Team consisting of:

- Director of Administration
- Head of Finance
- Chief of HR and Corporate Operations (who will make an initial assessment of the situation together with the IT Manager)
- Any Staff Member(s) involved in the real or potential breach of financial data
- IT Manager (if deemed appropriate/required by the Director of Administration, Head of Finance and Chief of HR and Corporate Operations)

In the absence of the Executive Director, the person responsible for the Organization must also be immediately notified. This person will (in case the Executive Director is unable to do this) immediately constitute the Crisis Management Team, undertake to oversee the coordination of the risk mitigation efforts and kept abreast of all developments (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Responsibility of the Chief of HR and Corporate Operations (or person responsible for the Organization in case of absence):

- Constitute a Crisis Management Team (involving those mentioned above);
- Ensure that appropriate people are involved in the investigation and risk mitigation work;
- Call for a detailed account of the data breach with specific information on the incident;
- Ensure that action is being taken promptly to address the issue and mitigate the risks;
- Actively participate in the risk assessment and mitigation processes;
- Ensure that a police report is filed (if appropriate);
- Inform themself of all actions being taken with regard to the matter.

Staff responsibility:

- Immediately inform both the Executive Director and Chief of HR and Corporate Operations (who will notify the Director of Administration) either in person or by telephone of the real or potential threat of compromised financial data. In the absence of both the Executive Director and Chief of HR and Corporate Operations, the Staff Member must also notify the person in charge of the Institute and notify the Executive Director as soon as possible either in person or by telephone thereafter.
- Provide comprehensive and detailed information to the Chief of HR and Corporate Operations that is required for the investigation and risk assessment in the form of a written report. At a minimum the information will contain:
    - What specific information was or is potentially compromised;

    - What specific form the information was in that was compromised (scans, hard copies, email access, etc.);
    - The specific circumstances including exact location, dates and times surrounding the event;
    - The name(s) of any person(s) involved in the event and a description of their specific involvement;
    - Action(s) (if any) already taken (specifying the person, date and time) to mitigate any potential risks.
- Failure by the Staff member(s) concerned with the event to provide an immediate report to the Executive Director and Chief of HR and Corporate Operations or to provide a full, detailed and accurate account of the circumstances surrounding the event may lead to disciplinary action.

Head of Finance responsibility:

- Obtain a list of all data that has been or could be compromised;
- Assess the level of intervention required;
- Where credit card information has been compromised, immediately contact the credit card company to register a fraud alert, obtain a list of any fraudulent activity and to cancel the credit card;
- Where a credit card has been cancelled – immediately notify all companies who have direct charging arrangements. The Finance Team maintains a comprehensive file for "Direct Charging Arrangements" containing details of all providers. In the event of a credit card being compromised, Finance will contact each provider;
- Where bank account information has been compromised, immediately contact the bank to notify them of potential risks, freeze the account and discuss with the bank the potential exposure once the account has been unfrozen. Depending on the crisis, it may be necessary to close the account and open a new account;
- In the event of a new bank account being opened, all organizations who pay directly into this account will need to receive new instructions;
- Where account information regarding the Endowment funds is compromised, immediately contact the Invstment Fund managers to notify them of the potential risks, and provide them with detailed information with respect to the information that was compromised. Request they perform a full risk and legal review of the information and the outcome of this review will inform the further action is required. If the Investment Fund managers advise that accounts are immediately frozen, both the Investment Fund Managers and the Head of Finance will need to contact each Portfolio Manager as soon as possible to freeze each account and change account numbers for each Fund. Once new account numbers have been established the accounts can be unfrozen;
- Where criminal activity has occurred, or is suspected to have occurred (for example an attempt to transfer funds), file a police report without delay.

IT Manager responsibility:

- Work with the relevant Staff to conduct investigations;
- Assist in risk assessment analysis if required and appropriate;
- Quickly put in place any IT solutions that can help to mitigate the risk;
- Before situations become crisis situations, increase user awareness on security issues by training Staff, conduct IT security risk assessments and put in place security measures to minimize potential security threats.

Notifying the parties involved

Determination of who to notify is based on the nature of the data that was accessed. Notification should occur in a manner that ensures the affected individuals/institutes will receive notice of the incident in a timely way so that they can, in turn take timely action to mitigate potential risks. Notification will be made in a timely manner, but not so soon so as to unnecessarily compound the initial incident with incomplete facts. In the case of real or potential breach of financial or

banking data, notification may need to be made to any or all of the following: the credit card company, the bank(s) or the Investment Fund managers.

2.2 Security breach involving other (non-financial) data

Notifications:
Any Staff Member who is aware of a data breach or IT security breach must immediately notify the Executive Director and Chief of HR and Corporate Operations (who will notify the Director of Administration) either in person or by telephone who, together, will make an initial assessment of the situation together with the IT Manager. Where financial/banking data may have been compromised, the Head of Finance must also be immediately notified (see section above regarding financial data breaches) and a Crisis Management Team put in place by the Executive Director.

As soon as an assessment has been made by the (Executive Director, Chief of HR and Corporate Operations and Director of Administration) and an action plan developed to mitigate potential risks, the Executive Director will be provided with regular updates on actions taken and any outcomes. In the absence of the Executive Director, the person responsible for the Institute must be immediately notified either in person or by telephone, and, if the situation so warrants (breach of financial/banking data) put in place the Crisis Management Team, undertake to oversee the coordination of the risk mitigation efforts and kept abreast of all developments (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Staff reporting responsibility:
The Staff Member who suspects the data breach must be prepared to provide the following information (verbally with immediacy and in writing as soon as possible thereafter) to the members of Management mentioned above:

- When (specific date and time) did the breach happen?
- How did the breach happen?
- What types of information were obtained? (types of data, specific files where known, whether the information was HR-related, financial/account-related or related to other data).
- What, if any, action has been taken to date to mitigate or investigate the matter?

Upon learning of a breach
A breach of data or suspected breach of data will be immediately investigated. Depending on the confidentiality of the information, only those Staff necessary for the data breach investigation will be informed of the data breach. Below is more information on the steps to be taken by management upon learning of a security breach.

Risk assessment
Once a breach has been verified, an assessment of the risks must be undertaken. This assessment should involve those individuals who are able to contribute to the risk assessment and to consider all aspects including:

- The sensitivity of the data that is compromised;
- The amount of data lost and the departments/persons affected;
- The likelihood that the data is usable or may cause harm;
- The likelihood that the data was intentionally targeted (increases chance for fraudulent use);
- The strength and effectiveness of the security measures in place that were protecting the information (e.g. encrypted information on a stolen device would greatly decrease chance of access);

- Ability to mitigate the risks (including likely measures that need to be taken).

Notifying the parties involved
Determination of who to notify is based on the nature of the data that was accessed. Notification should occur in a manner that ensures the affected individuals/institutes will receive notice of the incident in a timely way so that they can, in turn take timely action to mitigate potential risks. Notification will be made in a timely manner, but not so soon so as to unnecessarily compound the initial incident with incomplete facts. As mentioned above in the case of real or potential breach of financial or banking data, notification may need to be made to any or all of the following: the credit card company, the bank(s) or the Investment Fund managers. For breaches of financial data please refer specifically to the procedures detailed under Section 2.1 above.

Mitigating risks
Based on the risk assessment, a plan will be developed to mitigate the risks involved. The course of action will aim to minimize the effect of the initial breach and to prevent similar breaches from taking place. As indicated above, those affected must be notified as soon as possible so they can take their own steps to mitigate potential risk to the Organization or to themselves. The steps provided to affected individuals will depend on the nature of the data breach.

3. THREATS TO CROP TRUST RESOURCES OR PROPERTY/ASSETS

3.1 Loss or theft of office keys
3.2 Loss or theft of Crop Trust property (laptop or other equipment)

3.1 Loss or theft of office keys

Staff Members issued with keys to the building and to the internal offices are responsible for them at all times. In this regard, Staff must ensure that they exercise caution when carrying these keys and take reasonable precautions to protect them from loss and theft. Loss or theft of the keys poses a significant risk to the Organization and must be handled swiftly. Below are the procedures to be followed in case of loss or theft of official keys.

Notifications:
The Chief of HR and Corporate Operations and Corporate Operations Officer should be notified immediately either in person or by telephone. The Director of HR and Corporate Operations must then notify both the Director of Administration and the Executive Director either in person or by telephone. If either are travelling, then the person responsible for the Organization must be notified (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Staff responsibility:

- Lost or stolen keys (whether main door or interior electronic fob keys) must be reported as soon as they are discovered to be missing and **no later than 2 hours after discovery of loss or theft.** Reports should be made either in person or by telephone to the Chief of HR and Corporate Operations (and his/her absence to the Corporate Operations Officer), providing as much information about the item and the circumstances as possible. Failure to report a lost key within this period may result in disciplinary action.
- The Staff Member concerned must file a police report (specifying loss of the keys and which type of keys) as soon as it is discovered that the keys are lost or stolen and no later than 24 hours after discovery of loss or theft. Since the Organization's corporate property insurance policy covers theft of items only in case where the Staff Member has not been negligent, Staff are encouraged to ensure that the police report properly reflects the situation in which the keys were lost. Copy of the police report must be provided to the

Corporate Operations Office. Failure to provide a copy of the police report within this period may result in disciplinary action.
- The Staff Member must make every reasonable effort to locate the keys where possible (call or visit the locations visited where the keys could have been lost).
- In the case that the keys are found, the Staff Member must inform the Corporate Operations office.
- Where it is determined that loss of keys was due to Staff negligence, any costs for replacement of keys or costs incurred due to the loss of the keys will be charged to the Staff Member concerned.

Responsibility of the Chief of HR and Corporate Operations (or Corporate Operations Officer):
- In case of loss/theft of a key to the external door, the building owners must be notified immediately of the lost keys and requested to change the locks.
- In case of loss/theft of a key to the external door, the other building occupants must be notified (and alerted that the building owners will likely change the door locks).
- In case of loss/theft of a key to the external door, the insurance company must be notified immediately and presented with a copy of the police report (obtained from the Staff Member).
- In case of loss/theft of an internal fob key, the Chief of HR and Corporate Operations (or Corporate Operations Officer) must provide the IT Manager with the key number and request that the fob key be immediately de-activated.
- Corporate Operations Office will annotate the key-issuance records indicating that the key(s) were lost/stolen and obtain signature from the Staff Member concerned.

IT Manager responsibility:
- In case of an internal fob key – once provided with the fob key number they must immediately de-activate the key.

3.2 Loss or theft of Crop Trust property (laptop or other equipment)

Staff Members issued with laptops and other equipment, or who are given responsibility for such equipment (camera or video camera equipment, etc.) are responsible for them at all times. In this regard, Staff must ensure that they exercise caution when carrying such equipment and take reasonable precautions to protect them from loss, theft and damage (both while travelling or while in their possession in the Crop Trust offices). Loss or theft of laptops poses a significant risk to the Organization (since these Organization's data and financial security may be compromised) and therefore loss of these items must be handled swiftly. Below are the procedures to be followed in case of loss or theft of such equipment.

Notifications:
The Chief of HR and Corporate Operations should be notified immediately either in person or by telephone **as well as the IT Manager so that steps can be taken to immediately deactivate the device if necessary**. The Chief of HR and Corporate Operations must then notify both the Director of Administration and the Executive Director or if travelling, then the person responsible for the Institute must be notified (see relevant Administrative Circular currently in effect for up-to-date list). In all cases, the Executive Director should be notified as soon as possible thereafter.

Responsibilities:

Staff responsibility:
- Lost or stolen Crop Trust property (laptop or other equipment) must be reported as soon as it is discovered to be missing and no later than 2 hours after discovery of loss or theft. Reports should be made to the Chief of HR and Corporate Operations and to the Corporate Operations Officer)**as well as the IT Manager** either in person or by telephone

providing as much information about the item and the circumstances as possible. Failure to report a lost item within this period may result in disciplinary action.

- The Staff Member concerned must make a police report (specifying loss of the item as soon as it is discovered that the item has been lost or stolen and no later than 24 hours after discovery of loss or theft. Copy of the police report must be provided to the Corporate Operations Office. Since the Organization's corporate property insurance policy covers theft of items only in case where the Staff Member has not been negligent, Staff are encouraged to ensure that the police report properly reflects the situation in which the item was lost. Failure to provide a copy of the police report within this period may result in disciplinary action. The Corporate Operations office maintains inventory lists with serial numbers of phones, computers and other equipment. Where possible, the Staff Member should obtain he serial number of the item and ensure that this is included in the police report.
- The Staff Member must make every reasonable effort to locate the item where possible (call or visit the locations visited where the items could have been lost).
- In the case that the items are found, the Staff Member must inform the Corporate Operations office and must report any damage.
- As indicated in the ICT Policies and Procedures manual, where it is deemed that loss or damage to the item(s) was due to negligence on the part of the Staff Member, depending on the circumstances and the extent of the loss or damage the Staff Member may be responsible for all or part of the costs incurred to replace or repair the item. This decision will rest with the Executive Director.

Responsibility of the Chief of HR and Corporate Operations (or Corporate Operations Officer):

- In case of loss/theft of a mobile phone, laptop or other device that may contain data, the Chief of HR and Corporate Operations (or Corporate Operations Officer) must immediately check with the IT Manager to ensure they have been notified who will try to locate the device using the remote locator software;
- In the case of a laptop or other device containing data, the Chief of HR and Corporate Operations (or Corporate Operations Officer) will ensure that the IT Manager meets with the Staff Member concerned to assess the level of protection to the device, the data contained on the device and the level of risk with regard to comprised data.
- The Chief of HR and Corporate Operations (or Corporate Operations Officer) will notify the insurance company immediately and present a copy of the police report (obtained from the Staff Member)
- Corporate Operations Office will annotate the equipment-issuance records indicating that the item(s) were lost/stolen and obtain signature from the Staff Member concerned.

IT Manager responsibility:

- In case of laptop or other device containing data:
    - Meet with Staff Member concerned to assess the level of protection to the device, the data contained on the device and the level of risk with regard to comprised data.
    - Where data is compromised, notify the relevant department so that appropriate measures can be taken immediately (see Section 2). Issues surrounding compromised financial or banking data must be handled immediately and without delay (see section regarding Financial Data under Section 2.1). In this regard, the IT Manager will immediately notify the Executive Director (if not already notified), the Director of Administration and the Head of Finance (if not already notified).

See Section 2 above for procedures regarding addressing crises involving compromised data.

Non-Working Hours

There is a possibility that crises may occur before or after regular office hours, or on a holiday or a weekend. While the structure of this plan remains precisely the same, its implementation may vary necessarily depending on, e.g. available resources and personnel until proper officials can be notified. Until that time, however, the individuals assuming the most responsibility will necessarily be those officials/individuals of highest rank who are available at the time (refer to the Administrative Circular regarding person responsible for the institute during absence of Senior Management). These individuals should seek to follow as nearly as possible the guidelines discussed in this plan, while simultaneously making an effort to notify the officials who are identified in this manual as requiring notification of the situation so as to obtain verification or advice on their actions.