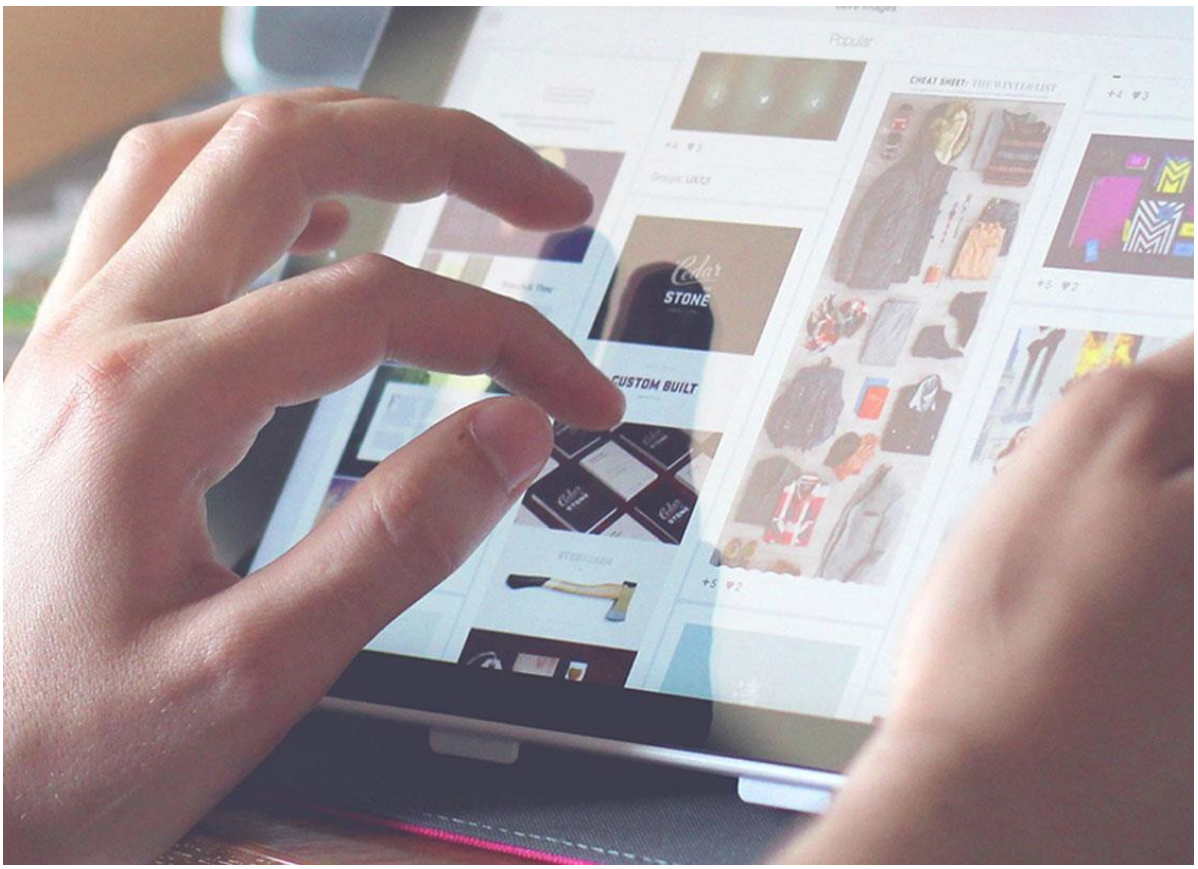
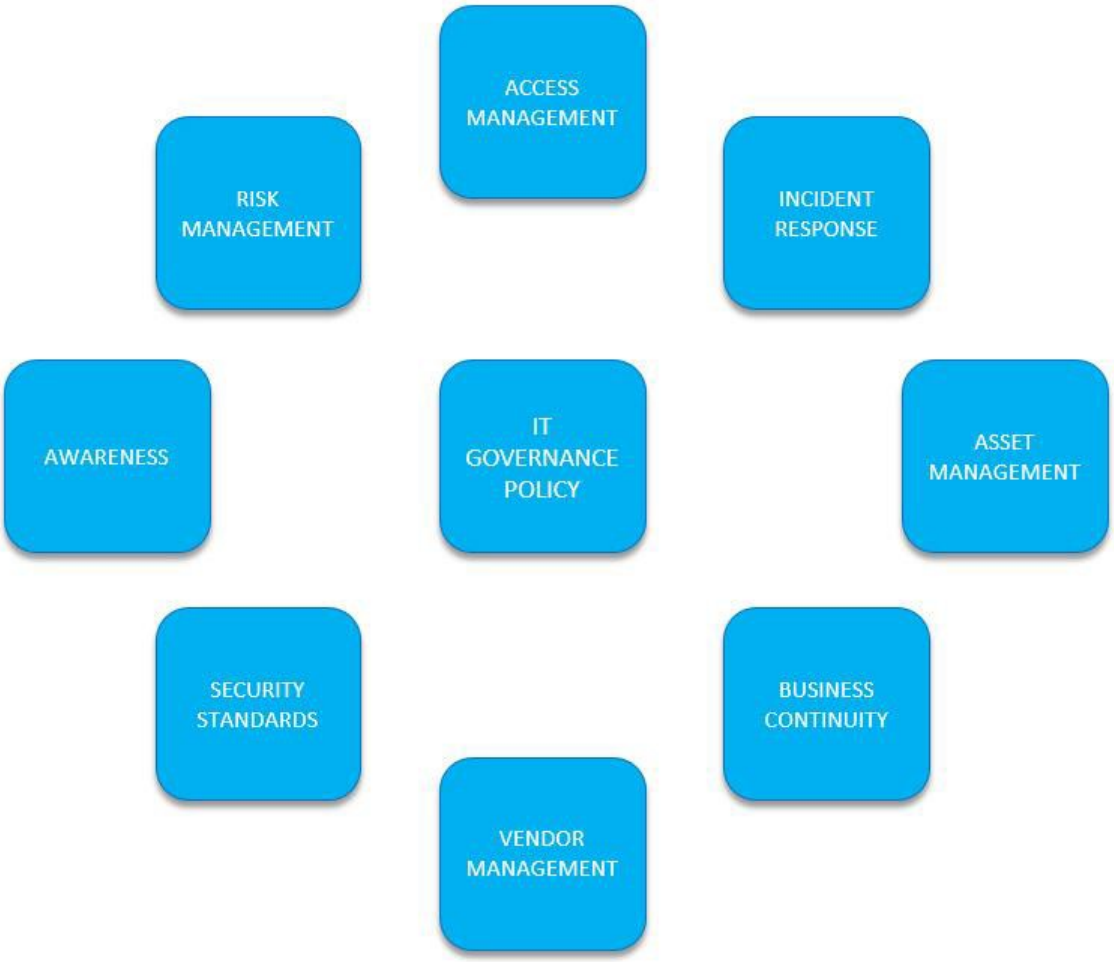
big easy | one
End to End Media Management



BIG EASY ONE IT GOVERNANCE POLICY 2020

big easy | one IT GOVERNANCE POLICY



IT Governance Policy

This document may be distributed to customers upon request when a relevant NDA is in force.

It does not include specific personnel, software or hardware

Contents

RISK MANAGEMENT.

1.1 *THE PROJECT WILL HAVE A PROJECT PLAN.*

1. *A process methodology will be applied throughout the project life cycle.*
2. *A systematic method of project tracking and control and a change control process will be used.*
3. *An acceptably detailed Work Breakdown Structure will be produced.*
4. *A proper status reporting mechanism will be used to update all interested parties.*
5. *All roles and responsibilities are defined.*

1.0POTENTIAL PROJECT RISKS: STAGE 1.

Item	*Low*	*Medium*	*High*
Acquisition of items critical to project success could be delayed in the procurement process			
Project schedule will exceed one fiscal year.			
Labour, support costs and other charges will increase from year to year.			
Project team member(s) will not be in place when required.			
Risks associated with using off-the-shelf packages.			
Risks associated with any conversions of existing data required before implementation of a new system.			
Can our development platform handle the workload required?			
Chance that the workstation environment of the intended user will change after requirements are gathered.			
Risks to the project caused by requirements that are inadequately defined.			
Chance that changes, in critical personnel on either the client or contractor side, will occur during the life of the project.			
Risk to the project of a facility move during the project			

Risks associated with personnel assigned to the project who may be pulled off anytime for another assignment			
Risk to cost and schedule involved with the use of subcontractors as a part of the development effort			
Chance that system owner or user support staff required to be available to the development team during the software development cycle will not be available.			
Risk caused by a system owner's or user's representative not participating in the change control process from the Requirements Definition Stage forward.			
Risk to the project resulting from a mandated/mandatory completion date for the project.			

2.0 POTENTIAL PROJECT RISKS STAGE 2.

Item	*Yes*	*No*
Elements of the project are being supplied by groups over which the project manager does not have direct control		
Two or more separate groups are developing parts of the software being delivered		
The development team is unfamiliar with the environment being used		
This is a first-time assignment for the project manager.		
The project is significantly larger or smaller than what the team is used to working on		
The project team has correct skills and can operate at the proper level to complete the needed work		
Additional skilled persons or resources are readily available in the event that problems occur on the project.		
Development and support groups are at different sites.		
The Project Plan accounts for vacation and sick leave by assigned personnel.		
The client or system owner supports a disciplined approach to software development, starting with a formal project plan.		
The project will receive the necessary level of support in terms of using repeatable processes (e.g., approvers will fully exercise their concurrence authority at stage exit		

AWARENESS TRAINING

1.1 *SENIOR PROJECT LEADER.*

1.0 ROLES.

i. *Use the information store chart to map & record all data types held within the business on individual PCs and test devices, internal network, Google drives, DropBox and AWS.*
ii. *Maintain & check scheme for allowable posts to social media*
iii. *Collect security poster & flyers and display on display boards.*

1.2 *PROJECT MANAGERS.*

2.0 ROLES

i. *Physically check movable media and devices into and out of the office daily.*
ii. *Keep check list on Google Drive*
iii. *Deliver security presentation jointly to new employees and updates at monthly team meetings & lunches.*

SECURITY STANDARDS

1.1 *NETWORK ADMINISTRATOR*

is designated to handle security and preparedness

1.0 ROLES

i. *Maintain list of information assets requiring protection,*
ii. *Maintain critical business functions computer equipment inventory*
iii. *Maintain and update cybersecurity incident response on 1st may & 1st October annually.*
iv. *Stay abreast of regulatory requirements regarding data security on 1st May & 1st October annually.*

2.0CONTROLLED NETWORK ACCESS

i. *Irregularly check, but at least weekly, all employee access logs.*
ii. *Maintain and review the firewalls and any breaches thereof.*
iii. *Maintain & review proxy server for internet access.*
iv. *Assign twelve digit minimum passwords and access controls to users and devices on the network.*
v. *Audit network connections monthly and eliminate unnecessary or outdated ones.*
vi. *Install updates and patches for operating systems and software immediately after consulting with Software Team lead.*
vii. *Maintain antivirus & antispyware; request review from business team for any attacks daily.*
viii. *Sensitive P2P file sharing may only be transferred via TABS*
ix. *Maintain encryption of all sensitive data files on all computers and storage devices including removable devices.*
x. *Review monthly ecommerce notes and security strategies from third party payment gateways.*
xi. *Ensure all data on hard-drives or movable devices is wiped using Gizmo or Secure Erase before disposal.*

1.2 *SENIOR PROJECT LEADER.*

1.0 ROLES.

i. *Use the information store chart to map & record all data types held within the business on individual PCs and test devices, internal network, Google drives, DropBox and AWS.*
ii. *Maintain & check scheme for allowable posts to social media*
iii. *Maintain employee departure checklist.*

1.3 *Project Managers.*

1.0 Roles

i. *Physically check movable media and devices into and out of the office daily.*
ii. *Keep check list on Google Drive*

VENDOR MANAGEMENT

1.1 *PROCUREMENT AND USAGE OF EXTERNAL THIRD PARTY RESOURCES*

2.0 PROCEDURE.

i. *Before researching possible third party suppliers check with Senior Team Lead or Senior Project Leader on whether it is necessary.*
ii. *Review Approved Vendor lists*
iii. *Review at least three competitors.*
iv. *Review complaints against vendors*
v. *Ask peer group for opinion*
vi. *Submit product and purchase approval from Senior Team Lead or Senior Project Leader*
vii. *Request purchase authorisation from Financial Control*
viii. *Take responsibility for performance monitoring and updates.*
ix. *Present results at monthly team meeting or lunch.*

BUSINESS CONTINUITY – ONSITE.

AS A TEAM MEMBER YOU SHOULD FAMILIARIZE YOURSELF WITH THIS PLAN.

1.2 *EMERGENCY NOTIFICATION CONTACTS*

Name	Address	Home Phone	Mobile/Cell Phone

1.3 *EMERGENCY RESPONSE ACTIVITIES*

	Action	Designated
1.	*Identify and assess network outage*	
2.	*Review with IT management*	
3.	*Evacuate area if necessary*	*Building security*
4.	*Initiate remedial actions to recover network assets*	*Lead network administrator or designee,*
5.	*Decision to invoke network DR plan*	
6.	*Initiate DR plan activities*	
7.	*Contact appropriate vendors and carriers*	
8.	*Follow through on recovery procedures*	
9.	*Report to senior IT management*	

1.4 *REVISIONS CONTROL PAGE*

Date	Summary of changes made	Changes made by

1.5 *TEAM MEMBER RESPONSIBILITIES*

Keep this list for reference at home in case a network disaster happens after normal work hours.

1.0 INVOCATION

If an initial assessment of the network disruption indicates a potentially prolonged outage (e.g., longer than eight hours), this plan becomes effective when approved by senior IT management. The plan will remain in effect until network operations are resumed at all affected locations.

2.0DISASTER DECLARATION

The Senior Management Team is responsible for declaring a disaster and activating network recovery as outlined in this plan.

3.0 NOTIFICATION

Regardless of the network disruption circumstances, the Senior Manager onsite must activate Disaster Recovery immediately in the following cases:

1. *Two or more systems and/or sites are down concurrently for three (3) or more hours.*
2. *Five or more systems and/or sites are down concurrently for three (3) or more hours.*
3. *Any problem involving a voice/data/Internet/wireless network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions is about to occur.*

4.0 EXTERNAL COMMUNICATIONS

The Senior Project Leader is principle contact for clients and other external organizations following a formal network disaster declaration.

5.0EMERGENCY MANAGEMENT STANDARDS

BACKUP POLICY

Full and incremental backups of projects, security information, system logs and technical documents should be stored on AWS in TABS project files as per information map.

Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation are stored with Managing Director

6.0 IT TECHNICAL SUPPORT DATA BACKUP AND ARCHIVING STANDARDS.

SYSTEM DATABASES

A copy of the most current network and system databases must be made at least weekly or based on frequency of changes made.

- *The lead network administrator is responsible for this activity.*

Offsite storage procedures

Media & data is stored in AWS cloud.
Access to backup databases and other data must be tested annually in second working week of January.

7.0 EMERGENCY MANAGEMENT PROCEDURES

In the event of any situation where access to a building housing network infrastructure equipment is denied, personnel should report to alternate locations or contact security for access if the location is not damaged or quarantined.

1.6 *ALTERNATE LOCATIONS*

Attempt to contact Managing Director or management via telephone. Home and cell phone numbers are (NOT) included in this document.

1.0 In the event of a natural disaster

In the event of a major catastrophe affecting network operations, immediately notify CIO +380977424844

2.0 In the event of a fire

If fire or smoke is present in the facility where network infrastructure assets are located, evaluate the situation and determine the severity, categorize the fire as a major or minor incident and take the appropriate action as defined in this section. Call 101 in Ukraine or 999 in UK

Step	Action
1	*Notify Managing Director impending event as time permits.*
2	*If impending natural disaster can be tracked, begin launching network DR plans within 48 hours as follows:* *Deploy network technical and admin personnel on standby.*
3	*24 hours prior to event:* • *Create an image of network and system databases and other relevant files.* • *Back up critical network and system elements.* • *Create backups VoIP systems, e-mail, routers, switches, file servers.*
	•

Attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers. Any other fire or smoke situation will be handled by building Security until the local fire department arrives.

In the event of a major fire, call 911 and immediately evacuate the area.

In the event of any emergency situation, such as system and network security, site security and personal safety are the major concerns. If possible, the lead network administrator and/or designee should remain present at the facility until the fire department has arrived.

3.0 IN THE EVENT OF A MAJOR CATASTROPHE AFFECTING THE FACILITY, IMMEDIATELY NOTIFY SENIOR MANAGEMENT.

Step	Actions
1	*101 - Fire,* *102 - Police,* *103 - Ambulance,* *104 - Gas .*
2	*Immediately notify all other personnel in the facility of the situation and evacuate the area.*
3	*Provide emergency services with your name, extension where you can be reached, building and room number, and the nature of the emergency. Follow all instructions given.*
4	*During non-staffed hours, security personnel will notify the Senior Executive responsible for the location directly.*
5	*Notify Building Security.* *Local security personnel will establish security at the location and not allow access to the site unless notified by the Senior Executive or designated representative.*
6	*Contact appropriate vendors to aid in the decision regarding the recovery and resumption of network services and protection of equipment as time and events permit.*
7	*All personnel evacuating the facilities will meet at their assigned assembly point and follow instructions given by the Senior Executive.* **Under no circumstances may you leave without the consent of a supervisor.**

4.0 NETWORK SERVICES PROVIDER OUTAGE

In the event of a network service provider outage, the guidelines and procedures in this section are to be followed.

STEP	ACTION
1	Notify Sys Admin of outage. Determine cause of outage and timeframe for its recovery.
2	If outage will be greater than one hour, route all calls via alternate services. If it is a major outage and all carriers are down and downtime will be greater than 12 hours, use the Managing Director's satellite phone

5.0 IN THE EVENT OF A FLOOD OR WATER DAMAGE

In the event of a flood or broken water pipe near any network infrastructure location, the guidelines and procedures in this section are to be followed.

Step	Action
1	Assess the situation and determine if outside assistance is needed; if this is the case, dial 101 immediately.
2	Immediately notify all other personnel of the situation and to be prepared to cease voice and data operations.
3	If water is slowly dripping from an air conditioning or ceiling and not endangering equipment, contact repair personnel / Building Security immediately.

6.0 PLAN REVIEW AND MAINTENANCE

This network disaster recovery plan must be reviewed on the first working day in August and January and exercised on the 10th working day of January.

Personnel listings and phone numbers should be main.

The electronic-copy version of the network DR plan is stored in TABS and on notice boards.

7.0 NETWORK DIAGRAMS

8.0 NOTIFICATION OF INCIDENT AFFECTING THE SITE

On-duty personnel responsibilities

<u>If in-hours:</u>

If you see a potentially serious network disruption, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate

<u>Out of hours:</u>

IT Technical Support personnel should contact CTO, Sys Admin, Managing Director.

BUSINESS CONTINUITY - SYSTEMS

1.1 *SYSTEMS STATUS*

Provide the following information when any of the following conditions exist:

I. *Network performance has sufficiently degraded to where normal operations are not possible for three or more hours.*
II. *Any problem at any network infrastructure asset, system or location that would cause the above condition to be present or there is certain indication that the above condition is about to occur.*

1.0 FACILITY STATUS

A. *Location of incident.*
B. *Type of incident (e.g., fire, hurricane, flood).*
C. *Summarize the damage (e.g., minimal, heavy, total destruction).*
D. *Meeting location that is a safe distance from the disaster scene.*
E. *An estimated timeframe of when a damage assessment group can enter the facility (if possible).*
F. *Contact the respective team leaders and report that a disaster involving network operations has occurred.*

2.0 INFORMING YOU OF DECISIONS

***If a disaster is not declared**, the location team will continue to address and manage the situation through its resolution and provide periodic status updates to Managing Director*

***If a disaster is declared**, IT Technical Support will immediately deploy network DR plans.*

***Declare a disaster** if the situation is not likely to be resolved within predefined time frames. The Managing Director will declare the disaster status.*

3.0 IT TECHNICAL SUPPORT WILL ASSESS THE DAMAGE TO THE NETWORK AND RELATED ASSETS.

Include vendors/providers of installed network services and equipment

A. *Participate in a briefing on assessment requirements, reviewing:*
   I. *Assessment procedures*
   II. *Gather requirements*
   III. *Safety and security issues*

B. Document assessment results

Building access permitting:

I. Conduct an on-site inspection of affected areas to assess damage to essential network records (files, manuals, contracts, documentation, etc.) and electronic data.

II. Obtain information regarding damage to the network, e.g., environmental conditions, physical structure integrity, furniture, and fixtures)

C. Recommendations for required resources.

Based on the information obtained, senior management will decide whether to continue to the business recovery phase. If the situation does not warrant this action, continue to address the situation at the building.

1.2 NETWORK RECOVERY

1.0 NOTIFY IT TECHNICAL SUPPORT STAFF AND COORDINATE RETURN TO PRIMARY FACILITY/LOCATION

2.0 SECURE FUNDING FOR RETURN TO WORK

Make arrangements in advance with network service carriers and equipment vendors to recover network operations.

3.0 NOTIFY NETWORK RECOVERY

Using the call list in Appendix B, notify the appropriate company personnel. Inform them of any changes to processes or procedures, contact information, hours of operation, etc.

4.0 OPERATIONS RECOVERED

Assuming all relevant network operations have been recovered either to the original location or to an alternate site with employees in place to support network operations, the company can declare that its network is functioning normally.

1.3 RECOVERY TEAM CONTACT LISTS

Name	Address	Home Phone	Mobile/Cell Phone

1.4 IT TECHNICAL SUPPORT

Name	Address	Home	Mobile

1.5 *FIRST RESPONDERS, NETWORK CARRIERS, PUBLIC UTILITY COMPANIES AND OTHERS*

Name	Contact Name	Phone
Fire,		*101 -*
Police,		*102 -*
Ambulance,		*103*
Gas		*104*

1.6 *INVENTORY OF BACKUP NETWORK SERVICES AND EQUIPMENT*

Device	Serial number/Model
Router board 750 GL Mikrotik	
WiFi router 802.11g with Ethernet, Zyxel model NBG334W EE	
Switch D-Link model DGS-1024A	
Switch D-Link model DES-1016D	
Everest PC	

1.7 *APPROVED VENDOR LIST*

5.0 SERVER AND COMPUTER EQUIPMENT SUPPLIERS

Company Name	Contact	Work	Mobile
Everest			
Rozetka.ua			
Computer world			

6.0 COMMUNICATIONS AND NETWORK SERVICES SUPPLIERS

Company Name	Contact	Work	Mobile

AWS			
RNC LLC			
Mirohost.net			
Skype	*Panel*		

ASSET MANAGEMENT

1.8 *SOFTWARE INVENTORY.*

Lists of all software on each machine and network is available on Google Drive
https://drive.google.com/drive/folders/0ByxIhhLXs8tmajY2cmZYNFI1V00

1.9 *LICENSE MANAGEMENT*

1.0 RESPONSIBILITY

Network Admin

i. *Provide monthly reportage on or around 10th of each calendar month*
ii. *Software licence compliance.*
iii. *Licence*

1.10 *SOFTWARE METERING*

1.0 RESPONSIBILITY

Network Admin

i. *Provide monthly reportage on or around 10th of each calendar month*
ii. *Utilisation of software*
iii. *Software licence compliance.*

1.11 *SOFTWARE DEPLOYMENT*

1.0 RESPONSIBILITY

Network Admin

i. *Best practice.*

ii. *Where possible use MSI not ZAP for Windows installations.*

iii. *Assigning applications to computers, not users.*

iv. *Maintain deployment list here and in recovery*

v. *Access Control List should be used to control Read permissions for unauthorised users*

1.12 *PATCH MANAGEMENT.*

i. *Follow Software Deployment best practice.*

1.13 *PRODUCT CATALOG.*

1.0 RECOMMENDED VENDORS

Windows.

Product	*Application*	*Vendor*	*Install date*	*Licence type*	*Licence number*	*Contact*
OS						
Management						
Design						
Comms						
VOIP						
Mail						

Development

OS						
Webserver						
Webserver						
Hypertext Interpretator						

DB						
IDE						
Framework						
Framework						
Framework						
Version control system						
Version control system						
Bug tracker						

INCIDENT RESPONSE

On discovery of an incident contact the following as appropriate.

Management

Name	Mobile/Cell Phone

Technical

Name	Mobile/Cell Phone

1.1 CLIENT DISCOVERY CONTACTS

A. *Helpdesk*

B. *Senior Project Leader*

C. *MD*

1.2 INTERNAL STAFF DISCOVERY

A. *System administrator / firewall administrator*

B. *Senior Manager*

i) *CTO*

ii) *MD*

iii) *Senior Project Leader*

List all sources and check off whether they have contact information and procedures. Usually each source would contact one 24/7 reachable entity such as a grounds security office. Those in the IT department may have different contact procedures than those outside the IT department.

1.3 *Senior Manager response*

1.0 Log

i. *The name of the caller.*

ii. *Time of the call.*

iii. *Contact information about the caller.*

iv. *The nature of the incident.*

v. *What equipment or persons were involved?*

vi. *Location of equipment or persons involved.*

vii. *How the incident was detected.*

viii. *When the event was first noticed that supported the idea that the incident occurred.*

2.0 Primary Assessment

i. *Is the equipment affected business critical?*

ii. *What is the severity of the potential impact?*

iii. *Name of system being targeted, along with operating system, IP address, and location.*

iv. *IP address and any information about the origin of the attack.*

3.0 Response team

Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.

i. *Is the incident real or perceived?*

ii. *Is the incident still in progress?*

iii. *What data or property is threatened and how critical is it?*

iv. *What is the impact on the business should the attack succeed? Minimal, serious, or critical?*

v. *What system or systems are targeted, where are they located physically and on the network?*

vi. *Is the incident inside the trusted network?*

vii. *Is the response urgent?*

viii. *Can the incident be quickly contained?*

ix. *Will the response alert the attacker and do we care?*

x. *What type of incident is this? Example: virus, worm, intrusion, abuse, damage.*

4.0 INCIDENT TICKET

Create an incident ticket& categorize as follows.

i. *Category one - A threat to public safety or life.*
ii. *Category two - A threat to sensitive data*
iii. *Category three - A threat to computer systems*
iv. *Category four - A disruption of services*

5.0 RESPONSE PROCEDURE

Team members will establish and follow one of the following procedures basing their response on the incident assessment:

i. *Worm response procedure*
ii. *Virus response procedure*
iii. *System failure procedure*
iv. *Active intrusion response procedure - Is critical data at risk?*
v. *Inactive Intrusion response procedure*
vi. *System abuse procedure*
vii. *Property theft response procedure*
viii. *Website denial of service response procedure*
ix. *Database or file denial of service response procedure*
x. *Spyware response procedure.*

If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

6.0 FORENSIC PROCESS.

Authorized personnel should:

i. *review system logs,*
ii. *look for gaps in logs,*
iii. *review intrusion detection logs*
iv. *interview witnesses and the incident victim to determine how the incident was caused.*

Recovery team

i. *recommend changes to prevent the occurrence from happening again or infecting other systems.*
ii. *Upon management approval, implement changes.*

iii. *Restore the affected system(s) to the uninfected state.*

Consider

i. *Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.*

ii. *Make users change passwords if passwords may have been sniffed.*

iii. *Be sure the system has been hardened by turning off or uninstalling unused services.*

iv. *Be sure the system is fully patched.*

v. *Be sure real time virus protection and intrusion detection is running.*

vi. *Be sure the system is logging the correct events and to the proper level.*

7.0 DOCUMENTATION

Document the following:

i. *How the incident was discovered.*

ii. *The category of the incident.*

iii. *How the incident occurred, whether through email, firewall, etc.*

iv. *Where the attack came from, such as IP addresses and other related information about the attacker.*

v. *What the response plan was.*

vi. *What was done in response?*

vii. *Whether the response was effective.*

Preserve Evidence

i. *make copies of logs, email, and other communication.*

ii. *Keep lists of witnesses.*

iii. *Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.*

Notifications

i. *Notify the police and other appropriate agencies if prosecution of the intruder is possible.*

Damage Assessment

ii. *Assess the damage to the organization*

iii. *Estimate both the damage cost and the cost of the containment efforts.*

Review response and update policies

i. *Plan and take preventative steps so the intrusion can't happen again.*

ii. *Consider whether an additional policy could have prevented the intrusion.*

iii. *Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.*

iv. *Was the incident response appropriate? How could it be improved?*

v. *Was every appropriate party informed in a timely manner?*

vi. *Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?*

vii. *Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?*

viii. *Have changes been made to prevent a new and similar infection?*

ix. *Should any security policies be updated?*

x. *What lessons have been learned from this experience?*

ACCESS MANAGEMENT

INTRODUCTION

The purpose of this policy is to prevent unauthorised access to the Bold Endeavours Group information systems. The policy describes the registration and de-registration process for all information systems and services.

These policies apply especially to new starters, leavers and those moving job, responsibility or Portfolio.

These policies should also be seen in the light of HR procedures to verify a new starters qualifications, references and employmentrights.

1.1 *APPROVAL AND AUTHORISATION*

1.0 CHANGE HISTORY

Version	Date	Reason
Draft 1.0	*01/01/2014*	*First draft for comments*
Version 1.0	*03/04/2014*	*First Version*
Version 1.1	*05/05/2015*	*Review & update*
Version 1.2	*05/05/2016*	*Review & update*
Version 1.3	*05/05/2017*	*Review & update*
Version 1.3	*05/05/2018*	*Review & update*
Version 1.5	*05/05/2019*	*Review & update*
Version 1.6	*05/01/2020*	*Review & update*

1.2 *USER REGISTRATION*

1.0 NEW USERS

Access to BE group information services is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.

Each user is identified by a unique user ID so that users can be linked to and made

responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out (ie. Training).

There is a standard level of access, document scanning, databases. Development servers, other services can be accessed when specifically authorised by HR/line management.

A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

- *Name of person making request*
- *Job title of the newcomers and workgroup*
- *Start date*
- *Services required (default services are: MS Outlook, MS Office and Internet access)*

Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure.

The user signs the form indicating that they understand the conditions of access.

Access to all BE systems is provided by IT and can only be started after proper procedures are completed .

A new user will be set up on receipt of written notification but not made available, by issue of password, until the individual's start date.

IT will maintain a record of all requests in a folder named "new users" in the Helpdesk, National mailbox and will file email paper copies in the user access file.

2.0 CHANGE OF USER REQUIREMENTS

Changed requirements will normally relate to an alteration to the applications used but may also involve network access. Requests must be in writing (e-mail or hard copy) and must be directed to the Helpdesk.

Changes will be made on receipt of a properly completed request, the same details as shown above are required and requests will be filed under "access change requests" in the Helpdesk, National mailbox.

The ISO will not normally be copied in on requests but must be consulted if the request is not for a standard network service.

3.0 CHANGE OF PASSWORD

Where a user has forgotten his/her password, the helpdesk is authorised to issue a replacement.

Upon receipt of such a request the Helpdesk will

1. *Ensure the request is logged.*
2. *Confirm the identity of the user by question about existing services/access or by reference to a work colleague*
3. *Issue a temporary, single use, password which will require the user to set up a formal password.*

4.0 REMOVAL OF USERS

As soon as an individual leaves the Trust's employment, all his/her system logons must be revoked.

As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

All notification will be filed in a folder called "Leavers" in the Helpdesk, National mailbox.

Additionally, IT operations will positively confirm leavers with HR, each Friday, retaining a copy of the e-mail and reply in a file "Leavers" in the Helpdesk, National mailbox, or hard copy in the user access file.

Unless otherwise advised, IT operations will delete network access for all leavers at 4pm each Friday (or on the leaving date if not a Friday) (old user ID's are removed and not re-issued). This will include access to all network services. IT operations will inform application owners of leavers where their systems are affected.

BE expects all leavers to hand over current files within their workgroup, however IT operations can move a leavers files to specific areas if requested. Normally a leaver's data will be left in its existing directory for one month and then archived off system (but can be recovered if required).

1.3 PRIVILEGE MANAGEMENT

"Special privileges" are those allowed to the system manager or systems programmers, allowing access to sensitive area (for example, passwords). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached

Privileged access must be authorised by the CIO using the request form shown in Appendix 1. All completed forms, both current and expired, will be held by the ISO who is authorised by the completed form to set up the access specified.

All requests for access outside normal services must be supported by a completed and authorised Privilege Access form.

The Director will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the ISO on a three monthly basis. The list will identify all separate logons for each system and service.

1.4 USER PASSWORD MANAGEMENT

Systems logon requires that all passwords be of a minimum of 12 characters.

*Temporary access may be granted on a need to use basis. Such logons may be granted but must be recorded and reported on the normal form. Temporary logons must be identified by a specific login (starting TEMP****) and must be deleted immediately after use.*

1.5 *REVIEW OF USER ACCESS RIGHTS*

A review of all network access rights at least twice a year, which is designed to positively confirm all users.

Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed.

Annually, there is a review of access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. All other logons will be deleted.

The review will be conducted as follows.

1. *Sys Admin will generate a list of users, by application.*
2. *The appropriate list will be sent to each Application owner who will be asked to confirm that all users identified are authorised to use the system.*
3. *Sys Admin will ensure a response.*
4. *Any user not confirmed will have his/her access to the system removed.*
5. *The ISO will maintain a file of -*
    a. *Lists sent over*
    b. *Application owner responses*
    c. *A record of action taken*
6. *The review will normally be conducted in August and January*

1.6 *APPENDIX 1 – REQUEST FOR PRIVILEGED ACCESS*

Name of applicant: _____

Job Title: _____

Access requested for:

Systems	Login Name	Access Level	Reason

Access required: **From date:** _____

To date: _____

Applicant signature: _____

Comments: _____

_____

System owner's authorisation: _____

Approved by:
CIO _____