Protective Marking, Handling and Disposal Policy

Table of Contents

REVISION HISTORY			
Issue	**Date**	**Changes**	**By**
1	July 2011	First Issue	CV
2	June 2012	Updated for Work Programme	JH
3	May 2013	Updated following 27001 stage 1, to add definitions of company confidential, client confidential & public information	JH
4	July 2015	Updated references DNCC to EMC	JH
5	Jan 2016	Updated job titles	JH
6	Jan 2019	Added reference to GDPR and changed terminology from work programme to Building Better Futures	JH

1. Introduction

EMC needs to protect information securely in line with the sensitivity of content and risk of disclosure.
The information will be labelled, stored, handled and disposed of, in accordance with relevant legislation.

2. Purpose

The policy defines how information used within EMC is to be security marked, handled and disposed of, for both paper and electronic media.
The Protective Markings do not impose any classification to restrict or to supply information under the Freedom of Information Act, Data Protection Act, General Data Protection Regulation or Environmental Information Regulations. However, they may indicate that all or some of the information may be subject to exemptions, for example personal information.

3. Scope

This policy applies to:

- All permanent employees;
- All temporary/contract employees employed or engaged by EMC;
- Workers/volunteers employed or engaged by EMC;
- All employees of partner or subsidiary organisations whilst at work and/or engaged on EMC business;
- Any other authorised users.
- Any reference in this document to "employee" is deemed to be a reference to any of the foregoing

4. Enforcement

The policies and security requirements in this document refer to and gain authority from the EMC Information Security Policy statement as authorised and issued by the EMC Chief Executive.

5. Policy

All information handled by the EMC has been classified as either:

- Company Confidential i.e. internal company information such as HR records, finance records, meeting minutes etc.
- Client Confidential i.e. records that contain individual's personal data, or member business information & contact details.
- Public Information i.e. marketing literature etc.

There is no requirement to apply protective marking to this information as all staff have been trained/briefed on how to handle these documents.

<u>In relation to the Building Better Futures / Employability Contracts there are specific requirements for marking of information as detailed in the following paragraphs:</u>

Protective Marking

All information for internal use will be protectively marked using the agreed markings detailed within this policy and must be used by all employees.

Employees must assess all information for a protective marking using the impact assessment in Appendix A, based on risk and impact of disclosure.

The protective markings to be used by employees are:

NOT PROTECTIVELY MARKED

Anyone can access the information internally or externally. It may be published on the web or in paper form (but may still be subject to copyright). There is no requirement to mark these documents.

PROTECT

Information where disclosure or unauthorised access would be inappropriate, inconvenient or cause harm or financial impact. There will be clear markings on the information as "PROTECT".

RESTRICTED

Information to be restricted at a higher level of assurance than Protect, due to significant inconvenience, damage, harm or financial impact on EMC or individuals. This marking applies to the holding, storage and transmission of bulk customer or employee records and access will be restricted. There will be clear markings on the information as "RESTRICTED".

All PROTECT and RESTRICTED information must be marked at the centre top or bottom of each page, with the relevant marking.

Protective markings must be reviewed during the life of the information or document to ensure the marking is appropriate and relevant. For example: A policy or management decision may be in draft form and marked "PROTECTED MANAGEMENT", but once ratified it may become available to all and the marking removed.

Building Better Futures / Employability Contracts
Customer files related to the Building Better Futures / employability contracts, where held in paper format, must be marked as 'RESTRICTED'. Hence the file is to be stamped or written 'RESTRICTED' in capital letters in the middle of the top & bottom of the folder. Any completed documents/letters which contain personal information e.g., copy of customer letters, completed Childcare Declaration form, completed Employment Start Declaration form, completed DWP forms etc., must be stamped or written 'RESTRICTED' in capital letters in the middle of the header & footer of the pages.

Handling

All information must be stored and handled appropriate to its protective marking, as detailed in Appendix A. Employees must not attempt to handle, store or transmit information by any means other than that defined for each Protective Marking within this policy Appendix A.

Transfer or transmission of RESTRICTED information must be authorised by the Information Asset Owner or delegated officer.

If employees receive or handle information that is marked by a more secure Government Protective Marking of CONFIDENTIAL, SECRET and TOP SECRET, they must discuss the issue immediately with Chief Executive who will advise.

Disposal

All information must be disposed of or sent to archive, in accordance with an approved retention and disposal schedule.

The destruction of information must be appropriate to its protective marking as detailed in Appendix A.

All redundant copies of EMC information classified as 'Protect' or 'Restricted' or above that has been generated in the course of printing, photocopying or handling such information, must be destroyed according to approved procedures.

It is the responsibility of the Information Asset Owner to ensure that procedures are followed to assure secure disposal of information when it is no longer required.

Where destruction of 'Protect' or 'Restricted' EMC information is given to a third party, this must be carried out by authorised EMC personnel or a EMC approved external destruction service.

When a third party is used for the disposal of EMC information, the third party must be contractually bound to employ security controls required by EMC.

Destruction of 'Protect' or 'Restricted' EMC information captured on electronic storage media must only be performed with methods and equipment approved by the IT Manager.

All data and software on EMC information system hardware or machine-readable media will be erased and made unrecoverable prior to reuse within EMC.

All data and software on EMC information system hardware or machine readable media will be erased and made unrecoverable prior to release to a third party for disposal, sale, service or repair.

EMC asset registers will include any devices that have been taken from service, sent for repair, used for parts or destroyed.

Policy Review
The Chief Executive will ensure that this policy is up-to-date and relevant

This policy has been approved by the Chief Executive.
Signed:

Title: Chief Executive
Date: January 2022

Appendix A - Handling, Storage, and Disposal Procedures for Building Better Futures / Employability Contracts

The table below defines how the information resource can be handled, transmitted, stored and disposed for the different security protective markings in use by EMC.

Internal applies for sending information within EMC, External applies for sending information outside of EMC to partners or third parties. Do not use a marking on correspondence sent to the public.

	NOT PROTECTIVELY MARKED	**PROTECT**	**RESTRICTED**
Handling:			
Document Marking	No marking required	"PROTECT" at the centre top or bottom of every page.	"RESTRICTED" at the centre top or bottom of every page.
Transmission:			
Email	EMC internal email or internet email – no marking required	**Internal**: EMC email marked PROTECT in the subject line using the disclaimer Only to be opened by addressee(s) or delegated employee Seek permission of the sender before forwarding or sending to other addresses **External using internet:** Encrypt information in an attachment Only use if the sender needs a reply, you are sure who is receiving it, and they consent to a reply via internet email.	**Internal:** EMC email marked RESTRICTED in the subject line plus relevant disclaimer of "Restricted" inserted. Only to be opened by addressee(s) Never forward or send to other addresses **External using internet:** **Never send via internet email**
Storage:			
Hard copy files	Relevant departmental hard copy storage areas	Lockable cabinets for hard copy.	Lockable cabinets for hard copy.
Electronic files	Relevant departmental electronic server files	Electronic server files to be restricted only to relevant staff who need to access the information as part of their roles.	Electronic server files to be restricted only to relevant staff who need to access the information as part of their roles.
Disposal:			
Hard copy files	General waste or recycling unless it contains personal data or business sensitive information, in which case it must be put in confidential waste	Confidential waste only	Confidential waste only
Electronic files	Deletion	Secure deletion / disposal	Secure deletion / disposal