CONTENTS

EXECUTIVE SUMMARY 3

FOREWORD 5

BASIC PRINCIPLES & KEY DEFINITIONS 6

01 PREPARING FOR A CYBER SECURITY INCIDENT 8

I. Draft a cyber security incident response plan and keep it up to date
II. Content of a cyber security incident response plan
III. Assigning responsibilities and creating a cyber security incident response team
IV. Call upon external experts
V. Equip your organisation to address a cyber security incident
VI. Prepare your communication strategy
VII. Cyber insurance

02 DETECTING AND IDENTIFYING POTENTIAL CYBER SECURITY INCIDENTS 19

I. Categories of incidents
II. Methods to detect incidents

03 HANDLING AN ACTUAL INCIDENT: CONTAIN, ERADICATE AND RECOVER 21

I. Convene your cyber security incident response team
II. Situational awareness
III. Containing a cyber security incident
IV. Eradication and clean-up
V. Recovery

04 COMMUNICATION DURING A CYBER SECURITY INCIDENT 26

I. Tools
II. Incident specific communication plan

05 INCIDENT FOLLOW-UP AND CLOSURE: LEARN FROM EACH INCIDENT! 30

I. Evaluation of lessons learned and future actions: organise a post-incident review
II. Incident tracking and reporting

GLOSSARY 32

BIBLIOGRAPHY 34

AKNOWLEDGEMENTS 35

ANNEX 36